POLYNOMIALS AND THEIR RESIDUE SYSTEMS

BY

AUBREY J. KEMPNER

(*Continued from page 266*)

III. Residual congruences and residue systems modulo m

§ 8. Reduced arithmetical sequences (modulo m)

We consider an arithmetical sequence of any order, $a_0, a_1, a_2, \cdots$, where all elements are integers, and reduce each term* modulo m (m a given positive integer), thus obtaining $\alpha_0, \alpha_1, \alpha_2, \cdots; 0 \leqq \alpha_i < m$. Similarly, the sequence of first differences is reduced modulo m, etc.—We introduce the following

Definition 7: *If the nth differences are all congruent to zero modulo m, but not all of the $n-1$st differences are congruent to zero, we call the arithmetical sequence $a_0, a_1, a_2, \cdots$ an arithmetical sequence of order n modulo m; and we call the sequence $\alpha_0, \alpha_1, \alpha_2, \cdots, 0 \leqq \alpha_i < m$, a reduced arithmetical sequence of order n, modulo m.*—When there is no danger of ambiguity, abbreviated terms explaining themselves are used.

It is clear that a given arithmetical sequence leads to exactly one reduced arithmetical sequence modulo m, while a given arithmetical sequence modulo m may be derived from any one of an infinite number of arithmetical sequences.

Theorem VIII: *A reduced arithmetical sequence is periodic.*

Proof: The general term of an arithmetical sequence of order n of which all elements are integers may be represented by a polynomial $f(x)$ of degree n, with fractional (including integral) coefficients, the denominators of which are factors of $n!$ (including $n!$ itself). Assume then the polynomial to be written in the form $f(x) = (1/k) \cdot p(x)$, where $p(x)$ is a polynomial with integral coefficients and k a factor of $n!$. Then

$$\frac{1}{k} \cdot p(x + k \cdot m) \equiv \frac{1}{k} \cdot p(x) \pmod{m}$$

for all integral x; and $k \cdot m$, and all the more $n! \cdot m$, is either the length of the period or a multiple of the length of the period.

---

* R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372, has discussed, in an entirely different field, interesting applications of more general sequences obtained by reducing (modulo a given integer k) the elements $u_0, u_1, u_2, \cdots$ of a sequence satisfying a recurrence relation $u_{x+k} + \alpha_1 u_{x+k-1} + \cdots + \alpha_k u_x = \alpha$, in which $\alpha, \alpha_1, \cdots, \alpha_k$ are given integers.

COROLLARY: *In case $k = 1$, that is, in case the polynomial representing the general term of the arithmetical sequence of order n has integral coefficients, the length of the period is a factor of the modulus m, including m itself.*

Assume now

$$\begin{array}{ccccccc} \alpha_{00} & \alpha_{01} & \alpha_{02} & \alpha_{03} & \cdots & & \\ \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} & \cdots & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{n0} & \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \cdots, & 0 \not\equiv \alpha_{n0} = \alpha_{n1} = \alpha_{n2} = \cdots, & \end{array}$$

to be a reduced arithmetical sequence modulo m of order n; then*

$$\alpha_{0k} \equiv \sum_{\nu=0}^{\nu=n} \binom{k}{\nu} \alpha_{\nu 0} \pmod{m}, \qquad \text{where} \qquad \binom{k}{0} = 1; \tag{8}$$

$$(-1)^k \cdot \alpha_{k0} \equiv \sum_{\nu=0}^{\nu=k} (-1)^\nu \binom{k}{\nu} \alpha_{0\nu} \pmod{m}. \tag{9}$$

Also, if $a_{00}, a_{01}, a_{02}, \cdots$ form an arithmetical sequence from which the reduced sequence in the α is obtained, and $a_{10}, a_{11}, a_{12}, \cdots$ the first differences, etc., then obviously

$$a_{0k} \equiv \sum \binom{k}{\nu} a_{\nu 0} \pmod{m}, \tag{8a}$$

$$(-1)^k \cdot a_{k0} \equiv \sum (-1)^\nu \binom{k}{\nu} a_{0\nu} \pmod{m}. \tag{9a}$$

THEOREM IX: *Assume $f(x)$ a polynomial with integral coefficients. The reduced arithmetical sequence modulo m derived from $\cdots f(-1), f(0), f(1), \cdots$ is of order lower than $\mu(m)$, where $\mu(m)$ is the number defined in* § 1.

Proof: The *reduced* sequence $\cdots \alpha_{-1}\, \alpha_0\, \alpha_1\, \alpha_2 \cdots$ is the same as if we had started, not from the polynomial $f(x)$, but from the corresponding, modulo m completely reduced, polynomial, which is of degree $< \mu(m)$.

* From the corresponding formulæ for arithmetical sequences of order n: $a_{00}, a_{01}, a_{02}, \cdots$. The second of these formulæ,

$$(-1)^k \cdot a_{k0} = \Sigma_{\nu=0}^{\nu=k} (-1)^\nu \cdot \binom{k}{\nu} a_{0\nu},$$

is obtained most directly by applying the first,

$$a_{0k} = \Sigma_{\nu=0}^{\nu=n} \binom{k}{\nu} a_{\nu 0},$$

to the arithmetical sequence obtained from the original sequence by replacing a_{ij} by $(-1)^{i+j} \cdot a_{ji}$, where now (on account of a_{ni} = constant), $a_{ji} = 0$ for $j > n$. (See § 10, end.)

COROLLARY: *Under the assumptions of the theorem, the* $\mu(m)$*th differences are all zero* ($\equiv 0 \pmod{m}$).

The theorem does *not* hold for arithmetical sequences whose elements are integers, but which are generated by polynomials with fractional, not integral, coefficients, as is shown by simple examples.

Example: $f(x) = 2 - \frac{5}{12}x + \frac{65}{24}x^2 - \frac{19}{12}x^3 + \frac{7}{24}x^4$ generates the arithmetical sequence of order four,

$$\begin{array}{ccccccccccc}
\cdots & 2 & 3 & 4 & 6 & 17 & 52 & 133 & \cdots \\
\cdots & 1 & 1 & 2 & 11 & 35 & 81 & 156 & \cdots \\
\cdots & 0 & 1 & 9 & 24 & 46 & 75 & 111 & \cdots \\
\cdots & 1 & 8 & 15 & 22 & 29 & 36 & 43 & \cdots \\
\cdots & 7 & 7 & 7 & 7 & 7 & 7 & 7 & \cdots
\end{array}$$

which reduces modulo 3 to a reduced sequence of order $4 > \mu(3)$ (but $\leqq n$):

$$\begin{array}{ccccccccc}
\cdots & 2 & 0 & 1 & 0 & 2 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 2 & 2 & 2 & 0 & 0 & \cdots \\
\cdots & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \cdots \\
\cdots & 1 & 2 & 0 & 1 & 2 & 0 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots.
\end{array}$$

In order to avoid ambiguity, and to express our theorems in the simplest form, we define residue systems in the following way:

DEFINITION 8: *Let* $f(x)$ *be a polynomial with integral coefficients (admitting as a polynomial also a constant either different from, or equal to, zero) and* m *a given positive integer. Then the numbers* $\alpha_i \equiv f(i) \pmod{m}$, $0 \leqq \alpha_i < m$, $i = 0, 1, 2, \cdots$, *starting always with* $i = 0$, *form a complete residue system modulo* m *of* $f(x)$.

Important in this definition are the words: "starting always with $i = 0$." Thus, $0, 0, 2, 1, 2, 0, 0, 2, 1, \cdots$ is a residue system modulo 5 of $x^2 - x$; but $0, 2, 1, 2, 0, 0, 2, 1, 2, \cdots$ is not a residue system of $x^2 - x$, but of, for example, $x^2 + x$.

We can already state, as a consequence of Theorem IX, the

COROLLARY: *The first* $\mu(m)$ *elements of a residue system modulo* m *of a polynomial with integral coefficients completely determine the whole residue system.* Only an obvious modification is required, in case any $\mu(m)$ consecutive elements are given.

This does not hold for polynomials which assume integral values for all integral x, but with rational (not integral) coefficients. We shall also see later that, except for m a prime, the $\mu(m)$ elements are not independent of each other.

§ 9. Simple applications of reduced arithmetical sequences

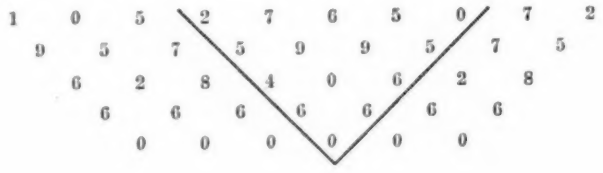
The preceding considerations permit a very simple treatment of the following problems.*

(*a*) Given a complete residue system modulo m; to determine the degree of the corresponding completely reduced polynomial.

Solution: We know that the degree is $< \mu(m)$. Determine $\mu(m)$. Form the sequence of first differences of the given residue system and reduce modulo m. If these differences are all zero, our function is a constant. If the ρth sequence of reduced differences (ρ necessarily $< \mu(m)$) is the first in which all elements vanish, the polynomial is of degree $\rho - 1$ exactly. In practice, one will make use of the fact that if in the $(\mu - 1)$st sequence of differences two consecutive elements are equal, then, since the (constant) μth difference is zero, all elements of the $(\mu - 1)$st sequence are equal; similarly, if there is a $k < \mu$ for which k consecutive elements of the sequence of differences of order $\mu - k + 1$ are equal, then all elements of this sequence vanish.

(*b*) Assume given consecutive residues modulo m, not necessarily starting from $f(0)$, but in sufficient number to determine the whole residue system. To complete the residue system and find the degree of the corresponding completely reduced polynomial.

Solution: The solution is obvious, by completing the sequence. For example, given modulo 10, $f(3) \equiv 2, f(4) \equiv 7, f(5) \equiv 6, f(6) \equiv 5, f(7) \equiv 0$.



We construct first the part of the table wedged in between the slanting lines. From this we see that our polynomial is of degree three, exactly. By completing the arrangement as indicated, we find the complete residue system to be

$$1\ 0\ 5\ 2\ 7\ 6\ 5\ 0\ 7\ 2.$$

(*c*) Given a complete residue system modulo m, or at least enough to determine it by (*b*). To determine the corresponding completely reduced polynomial.

Solution: We assume in the residue system at least $\mu(m)$ consecutive elements known. If these are the first $\mu(m)$ elements, then

$$\alpha_{0k} \equiv \sum_{\nu=0}^{\mu(m)-1} \binom{k}{\nu} \alpha_{\nu 0} \pmod{m}$$

determines a polynomial of the proper degree, and it remains to completely reduce this polynomial in case the coefficients do not satisfy the inequalities of § 5.

* In the treatment of these problems, the number $\mu(m)$ plays so natural a rôle that a method making systematic use of it may be expected to be somewhat simpler and shorter than methods where $\mu(m)$ is not explicitly employed. This is the justification for inserting these applications which are, on the whole, of the nature of simple interpolation problems.

Example: $f(4) \equiv 9, f(5) \equiv 16, f(6) \equiv 25, f(7) \equiv 6, f(8) \equiv 13, f(9) \equiv 4 \pmod{30}$. Since $\mu(30) = 5, f(x)$ is of degree $\mu - 1 = 4$ at most.

$$\begin{array}{ccccccc} 9 & 16 & 25 & 6 & 13 & 4 \\ & 7 & 9 & 11 & 7 & 21 \\ & & 2 & 2 & 26 & 14 \\ & & & 0 & 24 & 18 \\ & & & & 24 & 24 \end{array}$$

and

$$\phi(x) = 9 + 7\binom{x}{1} + 2\binom{x}{2} + 24\binom{x}{4} = 9 + 12x^3 - 6x^3 + x^4$$

is a polynomial for which, not as required, $f(4) \equiv 9, f(5) \equiv 16, \cdots \pmod{30}$, but instead $\phi(0) \equiv 9$, $\phi(1) \equiv 16, \cdots$ etc. To deduce the polynomial $f(x)$ from $\phi(x)$, we form first $g(x) = \phi(x-4)$ and reduce the coefficients modulo 30, thus obtaining $g(x) \equiv 1 + 20 \cdot x + 0 \cdot x^2 + 8 \cdot x^3 + 1 \cdot x^4 \pmod{30}$, where now, as required, $g(4) \equiv 9, g(5) \equiv 16, \cdots$. However, $g(x)$ is not a completely reduced polynomial modulo 30, since each such polynomial must be of the form: $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4, 0 \leqq a_0 < 30, 0 \leqq a_1 < 30, 0 \leqq a_2 < 15, 0 \leqq a_3 < 5, 0 \leqq a_4 < 5$, while in $g(x)$ we have $a_3 = 8$. In this case, where we need the individual completely reduced polynomial, it is necessary to reduce $g(x)$ by means of the explicit congruences $1 \cdot x(x-1)(x-2)(x-3)(x-4) \equiv 0, 5 \cdot x(x-1)(x-2) \equiv 0, 15 \cdot x(x-1) \equiv 0 \pmod{30}$. We find for our completely reduced polynomial $f(x) = 1 + 25x + 0x^2 + 3x^3 + 1x^4$, which satisfies the assumed conditions.

§ 10. Residual congruences modulo m of the second kind

We have seen that modulo m a residue system of a polynomial with integral coefficients is always completely determined by any $\mu(m)$ consecutive elements. By Definition 8, § 8, a residue system $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ is distinct from $\alpha_1, \alpha_2, \cdots, \alpha_{m-1}, \alpha_0$ or from any other one obtained from it by cyclic interchange; (the passage from the generating polynomial of the one to the generating polynomial of the other is given by replacing, in $f(x)$, x by $x - c$, where c is a certain integer. See problem (*c*) of § 9). By definition, always $\alpha_i \equiv f(i) \pmod{m}$.

Unless m is a prime, there exist relations between these $\mu(m)$ residues, as will soon be seen from the fact that the number of distinct residue systems modulo m is, unless m is a prime, smaller than $m^{\mu(m)}$, the number which we should obtain if the $\mu(m)$ residues $\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}$, which determine the whole residue system, were at liberty to range independently from 0 to $m - 1$. Our next problem is to establish these interrelations and generally to examine the structure of residue systems for a given modulus m.

We note first the obvious

LEMMA 9: *If p is any prime factor of the modulus m, and $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}, \alpha_m = \alpha_0, \alpha_{m+1} = \alpha_1, \cdots$ the complete residue system modulo m of a polynomial with integral coefficients, then $\alpha_{k+p} \equiv \alpha_k \pmod{p}$ for all integral k.*

From this follows immediately

LEMMA 10: *If d is any divisor of m containing no square factors* (i.e., $d = p_1 \cdot p_2 \cdots p_\rho$, $p_1 \neq p_2 \neq \cdots \neq p_\rho$), *then $\alpha_{k+d} \equiv \alpha_k \pmod{d}$ for all integral k.*

We continue with the following assertion:

Let $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, ($\alpha_i \equiv f(i) \pmod m$, $0 \leqq i < m$, $f(x)$ a polynomial with integral coefficients) be a complete residue system modulo m of $f(x)$, and let d be any divisor of m. Then

$$\alpha_{k+\mu(d)} - \binom{\mu(d)}{1} \cdot \alpha_{k+\mu(d)-1} + \binom{\mu(d)}{2} \cdot \alpha_{k+\mu(d)-2} - \cdots \pm \alpha_k \equiv 0 \pmod d \tag{10}$$

for $k = 0, 1, 2, \cdots, \mu(d) - 1$ and therefore for all integral k.

Proof: We reduce $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, modulo d. Since d is a divisor of m, we shall obtain the same result as if we had reduced directly modulo d the arithmetical sequence $f(0), f(1), \cdots, f(m-1)$, that is, we shall obtain the complete residue system modulo d of $f(x)$, but repeated m/d times over. By Theorem IX, § 8, the differences of order $\mu(d)$ are all zero ($\equiv 0 \bmod d$). Applying formula (9) of § 8, writing α_i for α_{0i} and taking $k = \mu(d)$, the statement is proved. Therefore, for each divisor, d, of m (including $d = m$), any element $\alpha_{k+\mu(d)}$ of a residue system modulo m is, at least modulo d, determined by the $\mu(d)$ p r e c e d i n g elements $\alpha_k, \cdots, \alpha_{k+\mu(d)-1}$, of the residue system. In the same way, of course, each element is determined, modulo d, by the $\mu(d)$ s u c c e e d i n g elements of the residue system.

The following notation suggests itself immediately:

$$\alpha_{k+\mu(d)} \equiv l(\alpha_{k+\mu(d)-1}, \alpha_{k+\mu(d)-2}, \cdots, \alpha_k) \pmod d \quad (k = 0, 1, 2, \cdots),$$

or, in order to save space and in close analogy with Definition 3 of § 2,

$$\alpha_{k+\mu(d)} \equiv l \pmod d \qquad (k = 0, 1, 2, \cdots), \tag{11}$$

where $l(\alpha_{k+\mu(d)-1}, \cdots, \alpha_k)$ and l each stand for: a n y l i n e a r p o l y n o m i a l i n $\alpha_{k+\mu(d)-1}, \cdots, \alpha_k$ w i t h i n t e g r a l c o e f f i c i e n t s w h i c h s a t i s f i e s f o r $k = 0, 1, 2, \cdots$ t h e c o n g r u e n c e (11). If we think of k as a variable and replace it by x, we have a congruence satisfied by all integral values of x, that is, exactly the kind of congruence considered in § 2 (the fact that x now does not assume negative integral values being due to the notation only), and we therefore write, using again the symbol $\equiv$,

$$\alpha_{x+\mu(d)} \equiv l \pmod d,$$

or, more conveniently for our purposes

$$\frac{m}{d} \cdot \alpha_{x+\mu(d)} \equiv l \pmod m,$$

and call such congruences again r e s i d u a l c o n g r u e n c e s, or, if we wish to distinguish them from the residual congruences introduced in

Part I, residual congruences of the second kind (modulo m). Finally, in order to indicate still more clearly by the notation the intimate relationship existing between these new residual congruences and those of Part I, we denote

$$\frac{m}{d} \cdot \alpha_{x+\mu(d)} \equiv l \bmod m$$

also by

$$\Big\}\mu(d), \frac{m}{d}\Big\{ \quad \text{or} \quad \Big\}\mu(d), \frac{m}{d}\Big\{_m \quad \text{or} \quad \Big\}\mu(d), \frac{m}{d}\Big\{ \pmod m.$$

We have thus proved

THEOREM X: *For any integer m and any factor d of m (including $d = m$, and, as a trivial case, $d = 1$), there exists a residual congruence of the second kind*

$$\alpha_{x+\mu(d)} - \binom{\mu(d)}{1} \cdot \alpha_{x+\mu(d)-1} + \binom{\mu(d)}{2} \cdot \alpha_{x+\mu(d)-2} - \cdots \pm \alpha_x \equiv 0 \pmod d,$$

or, using the notations introduced above,

$$(12) \qquad \alpha_{x+\mu(d)} \equiv l \pmod d, \qquad \text{or}^* \qquad \frac{m}{d} \cdot \alpha_{x+\mu(d)} \equiv l \pmod m,$$

or

$$(12) \qquad \Big\}\mu(d), \frac{m}{d}\Big\{, \qquad \text{or} \qquad \Big\}\mu(d), \frac{m}{d}\Big\{_m.$$

These residual congruences of the second kind are complete analoga of the residual congruences of § 2, and our considerations in Part III will go parallel with corresponding considerations of Part I, thus establishing a complete isomorphism between the structure of the totality of completely reduced polynomials modulo m and the totality of complete residue systems for the same modulus; such that every statement referring to the structure of the one totality leads immediately to a corresponding statement concerning the structure of the other.

The simple underlying reason for this parallelism may be indicated as follows: In an arithmetical sequence of order n,

$$\begin{array}{ccccccccccccc}
\cdot & \cdot & \cdot & a_{00} & a_{01} & a_{02} & \cdot & \cdot & \cdot & a_{0\lambda} & a_{0,\lambda+1} & \cdot & \cdot \\
\cdot & \cdot & \cdot & a_{10} & a_{11} & a_{12} & \cdot & \cdot & \cdot & a_{1\lambda} & a_{1,\lambda+1} & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & a_{n0} & a_{n1} & a_{n2} & \cdot & \cdot & \cdot & a_{n\lambda} & a_{n,\lambda+1} & \cdot & \cdot
\end{array},$$

with $a_{\rho,\sigma+1} - a_{\rho,\sigma} = a_{\rho+1,\sigma}$, and $0 \neq a_{n0} = a_{n1} = \cdots$, the formula (8):

* In the next congruence, all coefficients of l have m/d as a factor. This l is of course not identical with the l of the preceding congruence.

$a_{0k} = \sum_{\nu=0}^{\nu=n} \binom{k}{\nu} \cdot a_{\nu 0}$ expresses the values $a_{0i} = f(i)$ (and therefore also their residues modulo m, where m is a given integer), in terms of the coefficients of the expansion

$$f(x) = a_{00} + a_{10} \cdot \frac{x}{1} + a_{20} \cdot \frac{x(x-1)}{1 \cdot 2} + a_{30} \cdot \frac{x(x-1)(x-2)}{1 \cdot 2 \cdot 3} + \cdots,$$

that is, the residues of $f(x)$ modulo m are expressed in terms of the coefficients a_{i0}.

On the other hand, the formula (9): $(-1)^k \cdot a_{k0} = \sum_{\nu=0}^{\nu=k} (-1)^\nu \cdot \binom{k}{\nu} \cdot a_{0\nu}$, which gives the coefficients a_{k0} of $f(x) = \sum_{\nu=0}^{\nu=n} a_{\nu 0} \cdot \binom{x}{\nu}$ in terms of $f(i) = a_{0i}$, is nothing but (8) applied to the new arithmetical sequence

$$\begin{array}{cccccccccc}
\cdot & \cdot & \cdot & a_{00} & -a_{10} & a_{20} & -a_{30} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & -a_{01} & a_{11} & -a_{21} & a_{31} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & a_{02} & -a_{12} & a_{22} & -a_{32} & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{array},$$

and we see that (8) and (9) are (essentially) the same formula, only with a_{i0} (the coefficients of $\sum a_{\nu 0} \cdot \binom{x}{\nu}$) and a_{0i} (the functional values $f(i)$) interchanged. (Compare § 8, second footnote, and § 2, end of long footnote.)

§ 11. Chain of residual congruences of the second kind; signature of the second kind

For any given modulus m we may derive a set of residual congruences of the second kind by choosing all factors of m, including m itself, and deriving for each factor the corresponding congruence (12) of § 10. However, in general these congruences will form subsets such that all congruences of any particular subset are implied by one congruence of this subset. These dependent congruences we shall reject, and the set of congruences retained we call a "a chain of residual congruences of the second kind, modulo m," or, a "chain of residual congruences," as in § 3, when the difference between the former type of chain and the present type does not have to be emphasized.

We shall have in detail:

(*a*) $m = p$, p a prime. Our chain consists of none but a trivial congruence. The p elements of a residue system modulo p may be chosen at random, so that no relation exists between them.* To the sole congruence $1 \cdot x^p \equiv \psi(x) \pmod{p}$ or $\{p, 1\}$ of § 3 corresponds now the sole congruence $\alpha_{x+p} \equiv \alpha_x \pmod{p}$ or $\}p, 1\{$. The "signature of the second kind," which we define under (*b*) below, is denoted for the case $m = p$ by $S(p) = \binom{p}{1}$, or $\binom{p\ 0}{1\ p}$, using the same notation which was introduced for the signature in § 4.

* See reference to Zsigmondy in Introduction.

(*b*) $m = p_1 \cdot p_2 \cdot p_3 \cdots p_\tau$, $p_1 < p_2 < \cdots < p_\tau$ prime numbers. Remembering that $\mu(p_1 \cdot p_2 \cdots p_i) = p_i$ $(i = 1, 2, \cdots, \tau)$ we obtain (from Theorem X, § 10) the set of residual congruences of the second kind

$$\alpha_{x+p_i} \equiv l \pmod{(p_1 p_2 \cdots p_i)} \qquad (i = 1, 2, \cdots, \tau),$$

or

$$\}p_i, 1\{_{p_1 \cdot p_2 \cdots p_i}.$$

This chain may be written also in either one of the two forms

$$p_\tau \cdot p_{\tau-1} \cdots p_{i+1} \cdot \alpha_{x+p_i} \equiv l \pmod{m} \quad (i = 1, 2, \cdots, \tau),^*$$

or

$$\}p_i, (p_\tau \cdot p_{\tau-1} \cdots p_{i+1})\{_m \qquad (i = 1, 2, \cdots, \tau).$$

These chains correspond exactly to the chains of §§ 3, 4. The (for our purposes unimportant) functions l may in case (*b*) be simplified by using Lemma 9 and 10. See Example, below.

We introduce a symbol, the signature of the second kind of m. Since we shall show that its properties are abstractly identical with the characteristic properties of the signature of m introduced in § 4, we shall denote it by the same symbol $S(m)$, or, if we wish to distinguish it from the other signature, by $S'(m)$. Likewise, we shall ordinarily omit the words "of the second kind," and call both simply "signature of m," when there is no risk of confusion. Then $S'(p_1 \cdot p_2 \cdots p_\tau)$ is read off from the chain of residual congruences above in the same way in which $S(p_1 p_2 \cdots p_\tau)$ was read off in § 4:

$$S'(p_1 p_2 \cdots p_\tau) = S(p_1 p_2 \cdots p_\tau)$$

$$= \begin{pmatrix} p_\tau & p_{\tau-1} & p_{\tau-2} & \cdots & p_1 & 0 \\ 1 & p_\tau & p_\tau p_{\tau-1} & \cdots & (p_\tau p_{\tau-1} \cdots p_2) & (p_\tau p_{\tau-1} \cdots p_1) \end{pmatrix}$$

$$= \begin{pmatrix} p_\tau & p_{\tau-1} & p_{\tau-2} & \cdots & p_1 \\ 1 & p_\tau & p_\tau p_{\tau-1} & \cdots & (p_\tau p_{\tau-1} \cdots p_2) \end{pmatrix}.$$

Here the arbitrary entry 0, $(p_\tau p_{\tau-1} \cdots p_1)$ corresponds to the trivial congruence mentioned in the last footnote. As is clearly seen, our chain of residual congruences is completely determined by the signature of $p_1 p_2 \cdots p_\tau$. Each entry $(p_\tau \cdot p_{\tau-1} \cdots p_{i+1})$ in the second line of $S(p_1 p_2 \cdots p_\tau)$ gives the coefficient on the left side of one of the congruences, while the upper entry p_i gives us the number p_i of terms sufficient to insure that the product of any residue α by $p_\tau p_{\tau-1} \cdots p_{i+1}$ is completely determined by the following (or preceding) p_i residues.

* $i = 0$ would correspond to the trivial congruenec $(m/1) \cdot \alpha_{x+1} \equiv 0 \bmod m$.

Example:* $m = 2 \cdot 3 \cdot 5$; $\mu(2 \cdot 3 \cdot 5) = 5$.

$$\begin{aligned} &\alpha_{x+5} - 5\alpha_{x+4} + 10\alpha_{x+3} - 10\alpha_{x+2} + 5\alpha_{x+1} - \alpha_x \equiv 0 \pmod{30} \\ &5(\alpha_{x+3} - 3\alpha_{x+2} + 3\alpha_{x+1} - \alpha_x) \equiv 0 \pmod{30} \\ &5 \cdot 3(\alpha_{x+2} - 2\alpha_{x+1} + \alpha_x) \equiv 0 \pmod{30} \\ &5 \cdot 3 \cdot 2(\alpha_{x+1} - \alpha_x) \equiv 0 \pmod{30}, \end{aligned}$$

of which the last congruence is trivial. These congruences are written

$$\begin{aligned} &1 \cdot \alpha_{x+5} \equiv l \pmod{30} \qquad \{5, 1\{ \\ &5 \cdot \alpha_{x+3} \equiv l \pmod{30} \quad \text{or} \quad \{3, 5\{ \\ &5 \cdot 3\alpha_{x+2} \equiv l \pmod{30} \qquad \{2, 5 \cdot 3\{, \end{aligned}$$

omitting the trivial congruence. The signature is

$$S(2 \cdot 3 \cdot 5) = \begin{pmatrix} 5 & 3 & 2 \\ 1 & 5 & 5 \cdot 3 \end{pmatrix} = \begin{pmatrix} 5 & 3 & 2 & 0 \\ 1 & 5 & 5 \cdot 3 & 5 \cdot 3 \cdot 2 \end{pmatrix}.$$

Besides, the congruences $\alpha_{x+5} \equiv \alpha_x \pmod 5$, $\alpha_{x+3} \equiv \alpha_x \pmod 3$, $\alpha_{x+2} \equiv \alpha_x \pmod 2$ of Lemma 9, § 10, tell us—as an obvious result—that in any residue system modulo 30 any element is congruent modulo 5 to its fifth succeeding or preceding element; is congruent modulo 3 to its third succeeding or preceding element, etc. Similarly modulo 6, 10, 15, from Lemma 10.

(c) $m = p^\gamma$. We assume first

(c_1) $\gamma < p$. In this case we may again conveniently replace in the congruences of Theorem 10 the functions l by a simpler set. We show this by proving

LEMMA 11: *For $m = p^\gamma$, $\gamma < p$, the residual congruences*

$$\alpha_{x+k\cdot p} - \binom{k}{1}\alpha_{x+(k-1)\cdot p} + \binom{k}{2}\alpha_{x+(k-2)\cdot p} - \cdots \pm \binom{k}{1}\alpha_{x+p} \mp \alpha_x \equiv 0 \pmod{p^k} \tag{13}$$

hold for $k = 1, 2, \cdots, \gamma$.

Proof: For $k = 1$, obviously $\alpha_{x+p} \equiv \alpha_x \pmod p$; for $k = 2$, we shall have $\alpha_{x+2p} - 2\alpha_{x+p} + \alpha_x \equiv 0 \pmod{p^2}$, since, if $f(x)$ is a polynomial with integral coefficients (of degree n), then $F(x) = (1/p)\{f(x+p) - f(x)\}$, $F(x+p) = (1/p)\{f(x+2p) - f(x+p)\}$ are again polynomials (of degree $n-1$) with integral coefficients, and therefore

$$F(x+p) - F(x) = (1/p)\{f(x+2p) - 2f(x+p) + f(x)\} \equiv 0 \pmod p.$$

Similarly, the lemma is proved for the kth differences of $f(x)$, $k = 1, 2, \cdots, \gamma$.

DEFINITION 9: *We denote the congruence* (13) *by* $\alpha_{x+k\cdot p} \equiv l' \pmod{p^k}$, *in case we wish to emphasize the special character of* (13).

Here the l' are certain l (see Theorem X), but the accent is introduced to remind us that of the $k \cdot p$ elements of the residue system preceding (or

* Compare the examples of § 11 with those of § 4.

succeeding) any element $\alpha_{x+k\cdot p}$, only the k equidistant elements $\alpha_{x+(k-1)\cdot p}$, $\alpha_{x+(k-2)\cdot p}$, $\cdots$, α_{x+p}, α_x are involved in the congruence.

We thus obtain for $m = p^\gamma$, $\gamma < p$, the chain of residual congruences

$$p^i \cdot \alpha_{x+(\gamma-i)\cdot p} \equiv l' \pmod{p^\gamma} \qquad (i = 0, 1, \cdots, \gamma - 1).^*$$

This is again completely analogous to § 4. The signature, introduced as in case (*b*), coincides again with $S(m)$ of § 4:

$$S(p^\gamma) = \begin{pmatrix} \gamma\cdot p & (\gamma-1)\cdot p & \cdots & (\gamma-i)\cdot p & \cdots & p \\ 1 & p & \cdots & p^i & \cdots & p^{\gamma-1} \end{pmatrix}$$

$$= \begin{pmatrix} \gamma\cdot p & (\gamma-1)p & \cdots & (\gamma-i)\cdot p & \cdots & p & 0 \\ 1 & p & \cdots & p^i & \cdots & p^{\gamma-1} & p^\gamma \end{pmatrix}.$$

Example: $m = 5^4$; $\mu(5^4) = 20$. The chain of congruences is, written out in full:

$$\begin{aligned} \alpha_{x+20} - 4\cdot\alpha_{x+15} + 6\cdot\alpha_{x+10} - 4\cdot\alpha_{x+5} + \alpha_x &\equiv 0 \pmod{5^4} \\ 5(\alpha_{x+15} - 3\cdot\alpha_{x+10} + 3\cdot\alpha_{x+5} - \alpha_x) &\equiv 0 \pmod{5^4} \\ 5^2(\alpha_{x+10} - 2\cdot\alpha_{x+5} + \alpha_x) &\equiv 0 \pmod{5^4} \\ 5^3(\alpha_{x+5} - \alpha_x) &\equiv 0 \pmod{5^4}, \end{aligned}$$

or,

$$5^i \cdot \alpha_{x+5(4-i)} \equiv l', \quad \text{resp.} \quad 5^i \cdot \alpha_{x+5(4-i)} \equiv l \pmod{5^4}, \qquad (i=0,1,2,3)$$

or

$$\} 5(4-i), 5^i \{ \pmod{5^4} \qquad (i=0,1,2,3).$$

The signature is again

$$S(5^4) = \begin{pmatrix} 4\cdot 5 & 3\cdot 5 & 2\cdot 5 & 1\cdot 5 & 0\cdot 5 \\ 1 & 5 & 5^2 & 5^3 & 5^4 \end{pmatrix}.$$

Each of the congruences yields a number of distinct relations between the elements of any residue system modulo 5^4 (of a polynomial with integral coefficients). For example, the first congruence written out yields

$$\alpha_{20} - 4\cdot\alpha_{15} + 6\cdot\alpha_{10} - 4\cdot\alpha_5 + \alpha_0 \equiv 0 \pmod{5^4},$$

$$\alpha_{21} - 4\cdot\alpha_{16} + 6\cdot\alpha_{11} - 4\cdot\alpha_6 + \alpha_1 \equiv 0 \pmod{5^4}, \qquad \text{etc.},$$

where the elements of the residue system may be thought of as repeated periodically indefinitely in either direction.

In this example, and similarly in other cases, the full congruences may be chosen instead of the set (13), that is

$$\begin{aligned} \alpha_{x+20} - \tbinom{20}{1}\alpha_{x+19} + \tbinom{20}{2}\alpha_{x+18} - + \cdots - \tbinom{20}{1}\alpha_{x+1} + \alpha_x &\equiv 0 \pmod{5^4} \\ 5(\alpha_{x+15} - \tbinom{15}{1}\alpha_{x+14} + \tbinom{15}{2}\alpha_{x+13} - + \cdots + \tbinom{15}{1}\alpha_{x+1} - \alpha_x) &\equiv 0 \pmod{5^4} \\ 5^2(\alpha_{x+10} - \tbinom{10}{1}\alpha_{x+9} + \tbinom{10}{2}\alpha_{x+8} - + \cdots - \tbinom{10}{1}\alpha_{x+1} + \alpha_x) &\equiv 0 \pmod{5^4} \\ 5^3(\alpha_{x+5} - \tbinom{5}{1}\alpha_{x+4} + \tbinom{5}{2}\alpha_{x+3} - \tbinom{5}{2}\alpha_{x+2} + \tbinom{5}{1}\alpha_{x+1} - \alpha_x) &\equiv 0 \pmod{5^4}. \end{aligned}$$

This set has the same signature as (13), and will therefore lead to the same reductions for all purposes for which we shall use the system.

(c_2) $m = p^\gamma$, $\gamma \geqq p$. By making use of the properties of $\mu(m)$ derived in § 1, the considerations applied in (c_1) will now lead to the chain

* $i = \gamma$ corresponding to the trivial congruence.

$$\alpha_{x+p} \equiv \alpha_x \pmod{p}, \quad \text{or}$$
$$\alpha_{x+p} \equiv l' \pmod{p}, \quad \text{and similarly}$$
$$\alpha_{x+2p} \equiv l' \pmod{p^2},$$
$$\alpha_{x+ip} \equiv l' \pmod{p^i}, \qquad i < p,$$
$$\alpha_{x+p^2} \equiv l' \pmod{p^{p+1}}, \text{ not only modulo } p^p, \text{ since } \mu(p^p) = \mu(p^{p+1}) = p^2;$$
$$\alpha_{x+p^2+p} \equiv l' \pmod{p^{p+2}},$$
$$\alpha_{x+p^2+i\cdot p} \equiv l' \pmod{p^{p+i+1}}, \qquad i < p,$$
$$\alpha_{x+2p^2} \equiv l' \pmod{p^{2p+2}}, \text{ not only modulo } p^{2p+1};$$
$$\alpha_{x+\rho p^2} \equiv l' \pmod{p^{\rho(p+1)}}, \qquad \rho < p,$$
$$\alpha_{x+p^3} \equiv l' \pmod{p^{p^2+p+1}}, \text{ not only mod } p^{p(p+1)};$$

Making all moduli equal to p^γ, we shall have $\{\mu(p^\gamma), 1\}$; $\{\mu(p^{\gamma_1}), p^{\gamma-\gamma_1}\}$; $\cdots$; $\{\mu(p^{\gamma_i}), p^{\gamma-\gamma_i}\}$; $\cdots$; $\{\mu(p), p^{\gamma-1}\}$, all modulo p^γ, where $\gamma_1, \gamma_2, \cdots$ are determined as the largest integers for which, resp., $\mu(p^{\gamma_1}) = \mu(p^\gamma) - p$, $\cdots$, $\mu(p^{\gamma_i}) = \mu(p^\gamma) - ip$, $\cdots$. (Compare the parallel work in § 4, case 4.)

Introducing the symbol for the signature as in (*b*) of this section, we obtain the expression which we had found in § 4:

$$S(p^\gamma) = \begin{pmatrix} \mu(p^\gamma) & \mu(p^\gamma) - 1\cdot p & \cdots & \mu(p^\gamma) - ip & \cdots & 0 \\ 1 & p^\gamma/p^{\gamma_1} & \cdots & p^\gamma/p^{\gamma_i} & \cdots & p^\gamma \end{pmatrix}.$$

From this formula, $S(p^\gamma)$, $\gamma < p$, is obtained as a special case.

Example: $m = 3^{11}$; $S(3^{11})$ as in § 4, leading to the chain: $1\cdot\alpha_{x+27} \equiv l'$; $3\cdot\alpha_{x+24} \equiv l'$; $3^2\cdot\alpha_{x+21} \equiv l'$; $\cdots$; all modulo 3^{11}. Each congruence establishes, as in the last example, a large number of interrelations between the elements of the residue system modulo 3^{11} of any polynomial with integral coefficients.

(*d*) $m = p_1^{\gamma_1}\cdot p_2^{\gamma_2}\cdots p_\nu^{\gamma_\nu}$. We define for general m the chain of congruences of the second kind in such manner as to make it also for this case clear that the signature of the second kind is represented by the same symbol as the signature introduced in § 4. We know from Theorem X, § 10, that for every divisor d of m exists a congruence

$$\frac{m}{d}\cdot\alpha_{x+\mu(d)} \equiv l \pmod{m}, \qquad \text{or} \qquad \Big\}\mu(d), \frac{m}{d}\Big\{_m,$$

corresponding to a congruence

* Here, as in the following congruences, it is only for special purposes sometimes of advantage to use the l' instead of the l. The accent may be omitted throughout. (See (c_1)).

$$\frac{m}{d} \cdot x^{\mu(d)} \equiv \psi(x) \pmod{m}, \qquad \text{or} \qquad \left\{ \mu(d), \frac{m}{d} \right\}_m .$$

We define, always in analogy with §§ 3, 4, a "chain of residual congruences of the second kind," or, simply, a "chain" for m by the following

CONSTRUCTION: *For all divisors of m, namely $d_0 = m, d_1, d_2, \cdots, d_\tau = 1$, find the corresponding $\mu(d)$ and consider the couples of numbers $\mu(d)$, m/d. Each of these couples leads to a residual congruence, $\{\mu(d), m/d\}_m$. If for two divisors, d_ρ, d_σ of m, we have $\mu(d_\rho) = \mu(d_\sigma)$, we retain only the larger of the divisors d_ρ, d_σ, ignoring the other. We finally obtain in this manner a set of congruences, one for each of the distinct values $\mu(d_1), \mu(d_2), \cdots$, and these, arranged in decreasing order of magnitude of the μ, are defined to form the "chain of residual congruences of the second kind modulo m."*

The operations which we have thus performed on the number m are identical with those of "Construction" § 3. We next define (as already indicated in (*b*), (*c*), (*d*), above) the signature of m of the second kind by the same symbol

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_i) & \cdots & \mu(d_\tau) \\ 1 & \dfrac{m}{d_1} & \cdots & \dfrac{m}{d_i} & \cdots & \dfrac{m}{d_\tau} \end{bmatrix}$$

used for the signature in § 4, and call the signature of the second kind again simply the "signature of m."

We are now in a position to state the result derived in the present section as follows:

THEOREM XI: *For any given modulus m we determine*

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_i) & \cdots & \mu(d_\tau) \\ 1 & \dfrac{m}{d_1} & \cdots & \dfrac{m}{d_i} & \cdots & \dfrac{m}{d_\tau} \end{bmatrix}$$

as explained in § 4. The signature determines a chain of congruences, modulo m,

$$1 \cdot \left(\alpha_{x+\mu(m)} - \binom{\mu(m)}{1} \cdot \alpha_{x+\mu(m)-1} + \binom{\mu(m)}{2} \cdot \alpha_{x+\mu(m)-2} - + \cdots \pm \alpha_x \right) \equiv 0,$$

. . . . . .

$$\frac{m}{d_i} \cdot \left(\alpha_{x+\mu(d_i)} - \binom{\mu(d_i)}{1} \cdot \alpha_{x+\mu(d_i)-1} + \binom{\mu(d_i)}{2} \cdot \alpha_{x+\mu(d_i)-2} - + \cdots \pm \alpha_x \right) \equiv 0,$$

. . . . . .

$$\frac{m}{1} \cdot (\alpha_{x+1} - \alpha_x) \equiv 0,$$

or, using the notation of Theorem X, § 10,*

* For many purposes, only the quantities $\mu(d_i)$ and m/d_i taken from our congruences are required, that is, exactly the information furnished by the signature. We also remember that in some cases the full congruences of Theorem XI may be simplified, as in (*b*), (*c*) of this section.

$$\frac{m}{d_i}\cdot\alpha_{x+\mu(d_i)}\equiv l \pmod m \qquad or \qquad \left.\begin{matrix}\mu(d_i),\\ \dfrac{m}{d_i}\end{matrix}\right\}_m \quad (i=0,1,\cdots,\tau).$$

We have now proved that, while the signature of the second kind has an entirely different meaning from the signature as defined in Part I, yet they may be represented by the same symbol $S(m)$. Moreover, this symbol governs certain operations, notably the formation of the "chains of residual congruences" of Part I and of the "chains of residual congruences of the second kind," and, while these two kinds of chains have different meanings and deal with entirely different objects, yet the operations in the two cases are formally identical.

Example: $m=5^4\cdot 7^3$. $\mu(5^4\cdot 7^3)=21$,

$$S(5^4\cdot 7^3)=\begin{pmatrix}21 & 20 & 15 & 14 & 10 & 7 & 5 & 0\\ 1 & 7 & 5\cdot 7 & 5^2\cdot 7 & 5^2\cdot 7^2 & 5^3\cdot 7^2 & 5^3\cdot 7^3 & 5^4\cdot 7^3\end{pmatrix},$$

$1\cdot\alpha_{x+21}\equiv l$; $7\cdot\alpha_{x+20}\equiv l$; $5\cdot 7\cdot\alpha_{x+15}\equiv l$; $5^2\cdot 7\cdot\alpha_{x+14}\equiv l$; $5^2\cdot 7^2\cdot\alpha_{x+10}\equiv l$; $5^3\cdot 7^2\cdot\alpha_{x+7}\equiv l$; $5^3\cdot 7^3\cdot\alpha_{x+5}\equiv l$, all modulo $5^4\cdot 7^3$; or $\}21,1\{$; $\}20,7\{$; $\}15,5\cdot 7\{$; $\}14,5^2\cdot 7\{$; $\}10,5^2\cdot 7^2\{$; $\}7,5^3\cdot 7^2\{$; $\}5,5^3\cdot 7^3\{$ mod $5^4\cdot 7^3$.

Similarly, the chain of congruences of the second kind for $m=2^7\cdot 3^4\cdot 7^2$ may be read off immediately from $S(2^7\cdot 3^4\cdot 7^2)$, as given in § 4.

§ 12. Complete residue systems modulo m; the characteristic $C(m)$

We make use of the "chain of congruences" of the preceding paragraph in the following manner. For a given m let $\alpha_0,\alpha_1,\alpha_2,\cdots,\alpha_{m-1}$ be a residue system (that is $0\leqq\alpha_i<m$, $f(i)\equiv\alpha_i \pmod m$, $f(x)$ a polynomial with integral coefficients). We divide by vertical bars our system into subsets containing respectively $\mu(d_\tau)$, $\mu(d_{\tau-1})-\mu(d_\tau)$, $\mu(d_{\tau-2})-\mu(d_{\tau-1})$, $\cdots$, $\mu(m)-\mu(d_1)$, $m-\mu(m)$ terms, starting from, and including, α_0:

$$\left|\begin{matrix}\alpha_0,\alpha_1\cdots\alpha_{\mu(d_{\tau-1})-1}\\ \mu(d_{\tau-1})\end{matrix}\right|\left|\begin{matrix}\alpha_{\mu(d_{\tau-1})}\cdots\alpha_{\mu(d_{\tau-2})-1}\\ \mu(d_{\tau-2})-\mu(d_{\tau-1})\end{matrix}\right|\cdots\left|\begin{matrix}\alpha_{\mu(d_i)}\cdots\alpha_{\mu(d_{i-1})-1}\\ \mu(d_{i-1})-\mu(d_i)\end{matrix}\right|$$

$$\cdots\left|\begin{matrix}\alpha_{\mu(d1)}\cdots\alpha_{\mu(m)-1}\\ \mu(m)-\mu(d_1)\end{matrix}\right|\left|\begin{matrix}\alpha_{\mu(m)}\cdots\alpha_{m-1}\\ m-\mu(m)\end{matrix}\right|,$$

where the second line indicates the number of elements contained in each subset.

By the first congruence of our chain, $1\cdot\alpha_{x+\mu(m)}\equiv l \pmod m$, every element after the $\mu(m)$th, that is, all elements $\alpha_{\mu(m)},\alpha_{\mu(m)+1},\cdots,\alpha_{m-1}$ are completely determined by the first $\mu(m)$ elements $\alpha_0,\cdots,\alpha_{\mu(m)-1}$, since, by assigning to x the value 0, we obtain from $\alpha_0,\cdots,\alpha_{\mu(m)-1}$ the value of $\alpha_{\mu(m)}$; then, from the same congruence, for $x=1$, we obtain from $\alpha_1,\cdots,\alpha_{\mu(m)}$ the value of $\alpha_{\mu(m)+1}$, etc., such that any $\mu(m)$ consecutive elements determine all of the rest. By the second congruence $(m/d_1)\cdot\alpha_{x+\mu(d_1)}\equiv l \pmod m$, each

of the $\mu(m) - \mu(d_1)$ elements $\alpha_{\mu(d_1)} \cdots \alpha_{\mu(m)-1}$ is *partly* determined by the $\mu(d_1)$ first elements, namely modulo d_1, so that, if the $\mu(d_1)$ first elements are fixed, each of the $\mu(m) - \mu(d_1)$ next elements have only m/d_1 among the values $0 \cdots m-1$ to range over. Similarly, by the third congruence, each of the $\mu(d_1) - \mu(d_2)$ elements $\alpha_{\mu(d_2)}, \cdots, \alpha_{\mu(d_1)-1}$ is determined modulo d_2, so that each has but m/d_2 of the values $0 \cdots m-1$ to range over. Finally, using each congruence in this way, the last one,* $(m/d_{\tau-1}) \cdot \alpha_{x+\mu(d_{\tau-1})} \equiv l \bmod m$, tells us that, if the $\mu(d_{\tau-1})$ first elements $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})}$ are known, then the next $\mu(d_{\tau-2}) - \mu(d_{\tau-1})$ elements, $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$, are determined modulo $d_{\tau-1}$, leaving each one of these elements $m/d_{\tau-1}$ of the values $0, \cdots, m-1$ to range over.

We have so far subjected each element of the residue system following the first $\mu(d_{\tau-1})$ elements, that is, we have subjected each of the elements $\alpha_{\mu(d_{\tau-1})}, \alpha_{\mu(d_{\tau-1})+1}, \cdots, \alpha_{m-1}$, to *one* of the congruences of the chain. Thus, $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$ have been subjected *only* to $\{\mu(d_{\tau-1}), m/d_{\tau-1}\}_m$; while similarly $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$ have been subjected *only* to $\{\mu(d_{\tau-2}), m/d_{\tau-2}\}$; $\alpha_{\mu(d_{\tau-3})}, \cdots, \alpha_{\mu(d_{\tau-4})-1}$ only to $\{\mu(d_{\tau-3}), m/d_{\tau-3}\}$; and so forth. In reality, however, $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$ are affected not only by $\{\mu(d_{\tau-2}), m/d_{\tau-2}\}$, but also by $\{\mu(d_{\tau-1}), m/d_{\tau-1}\}$; $\alpha_{\mu(d_{\tau-3})}, \cdots, \alpha_{\mu(d_{\tau-4})-1}$ are affected not only by $\{\mu(d_{\tau-3}), m/d_{\tau-3}\}$, but also by $\{\mu(d_{\tau-2}), m/d_{\tau-2}\}$ and $\{\mu(d_{\tau-1}), m/d_{\tau-1}\}$, etc. *We shall show*† *in* § 13 *that the* α_i *are not any farther restricted by these additional considerations*, so that:

the number of values among the numbers $0, 1, \cdots, m-1$ left available for each of $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$, after $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ have been arbitrarily chosen (from $0, 1, \cdots, m-1$), is *exactly* $m/d_{\tau-1}$;

the number of values available for each of $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$, after the $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ have been arbitrarily chosen and the $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$ have been chosen subject to (1), is *exactly* $m/d_{\tau-2}$; etc.; generally:

the number of values available for $\alpha_{\mu(d_i)}, \cdots, \alpha_{\mu(d_{i-1})-1}$, after $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ have been arbitrarily chosen, after $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$ have been chosen subject to (1), $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$ subject to (2), etc., is *exactly* m/d_i.

We continue our discussion under the assumption of this at present not completely proved statement.

We are thus led, for any modulus m, to an arrangement of the following type, where in the first line the range of the index ν of the elements α_ν is given

* Omitting the trivial one $\{1, m/d_\tau\}$, $d_\tau = 1$.

† By proving that the present restrictions on the α_i are already sufficient to reduce the possible number of residue systems modulo m to its true number (see § 13, Theorem XIII, proof).

for each subset of the alpha's, while in the second line is entered for each subset the number of values over which each alpha of the subset is allowed to range:

$$\begin{matrix} 0 \cdots \mu(d_{r-1}) - 1 \\ m \end{matrix} \left| \begin{matrix} \mu(d_{r-1}) \cdots \mu(d_{r-2}) - 1 \\ m/d_{r-1} \end{matrix} \right| \cdots \left| \begin{matrix} \mu(d_i) \cdots \mu(d_{i-1}) - 1 \\ m/d_i \end{matrix} \right|$$

$$\cdots \left| \begin{matrix} \mu(d_1) \cdots \mu(m) - 1 \\ m/d_1 \end{matrix} \right| \begin{matrix} \mu(m) \cdots m - 1 \\ 1 \end{matrix}.$$

We replace in the first line $0 \cdots \mu(d_{r-1}) - 1$ by the number of elements contained in this subset, that is, by $\mu(d_{r-1})$, and similarly for the other subsets, and are led to the

DEFINITION 10: *To every positive integer m corresponds a symbol $C(m)$, which we call the characteristic of m of the second kind, or, since it is represented by the same symbol which was introduced for the characteristic of § 5, simply the characteristic of m. $C(m)$ is defined as*

$$C(m) = \left(\begin{matrix} \mu(d_{r-1}) \\ m \end{matrix} \left| \begin{matrix} \mu(d_{r-2}) - \mu(d_{r-1}) \\ m/d_{r-1} \end{matrix} \right| \cdots \left| \begin{matrix} \mu(d_{i-1}) - \mu(d_i) \\ m/d_i \end{matrix} \right| \right.$$

$$\left. \cdots \left| \begin{matrix} \mu(d_1) - \mu(d_2) \\ m/d_2 \end{matrix} \right| \begin{matrix} \mu(m) - \mu(d_1) \\ m/d_1 \end{matrix} \right).$$

In this symbol the first line gives the number of those elements of the residue system modulo m of any polynomial with integral coefficients which are contained in the successive subsets described above, while the lower line gives the number of numbers of the set $0, 1, 2, \cdots, m-1$ over which each element of the respective subset may range.

We know that $C(m)$ of Part I, and therefore also $C(m)$ of the present part, can be written down in all cases directly from $S(m)$, which, in turn, is derived from m by a simple and direct process.

§ 13. The number $N(m)$ of complete residue systems modulo m. Discussion of the totality of residue systems modulo m

THEOREM XII: *For a given modulus m the number of residue systems $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, $0 \leqq \alpha_i < m$, is $N(m)$.* (For definition of $N(m)$, see § 6.)

Proof: To every polynomial (with integral coefficients) corresponds *one* residue system $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, and to no two *completely reduced* polynomials corresponds the same residue system unless corresponding coefficients be equal (or their difference would be a polynomial congruent to zero modulo m for all integral values of the argument, thus leading to a contradiction of Theorem IV of § 5 and the lines preceding the theorem. Therefore the number of

residue systems modulo m is $N(m)$, the number of completely reduced polynomials.

THEOREM XIII: *A set of m integers $\alpha_0, \cdots, \alpha_{m-1}$, $0 \leqq \alpha_i < m$, forms a residue system modulo m of a polynomial with integral coefficients when and only when the chain of congruences of* § 11 *is satisfied.*

Proof: We know from § 12 that the condition is *necessary.* To show that it is also *sufficient,* we argue as follows:

(*a*) The true number of residue systems modulo m is $N(m)$ (Theorem XII).

(In particular, therefore, the formulæ of § 6 for $N(m)$ (for the general case as well as for the special cases) hold for the number of residue systems. We have thus a simple direct method of determining this number for any given modulus m.)

(*b*) We know that in the discussion of § 12 we have possibly left too large a range of values for the α_i, since we are not certain that we have exhausted the force of the chain of congruences $\{\mu(d_i), m/d_i\}$; therefore the number,—say $N'(m)$,—which we obtain by considering only the restrictions indicated in § 12, satisfies $N'(m) \geqq N(m)$ (the true number).

(*c*) It is easily shown that we obtain the right number $N(m)$ of residue systems by admitting just the congruential restrictions considered in § 12. We conclude this from the parallelism between the characteristic $C(m)$ of the first kind and the characteristic $C'(m)$ of the second kind. Both are denoted by

$$\left(\begin{matrix}\mu(d_{\tau-1}) \\ m\end{matrix}\middle|\begin{matrix}\mu(d_{\tau-2})-\mu(d_{\tau-1}) \\ m/d_{\tau-1}\end{matrix}\middle|\cdots\middle|\begin{matrix}\mu(d_{i-1})-\mu(d_i) \\ m/d_i\end{matrix}\middle|\cdots\middle|\begin{matrix}\mu(m)-\mu(d_1) \\ m/d_1\end{matrix}\right).$$

For the completely reduced polynomials we recall that $C(m)$ informs us that there are (certain) $\mu(d_{i-1}) - \mu(d_i)$ coefficients which range independently over m/d_i values $0, \cdots, (m/d_i) - 1$, thus leading to the expressions for $N(m)$ given in Theorem V. For the residue systems, $C(m)$ informs us that there are (certain) $\mu(d_{i-1}) - \mu(d_i)$ elements α which may each assume m/d_i values from among the numbers $0, \cdots, m-1$. These values are determined by the congruences of the chain. By referring to § 12, beginning, it is clear that we thus obtain exactly the expression obtained in § 6 for $N(m)$. Therefore $N'(m) = N(m)$.

(*d*) Therefore every one of the $N(m)$ sets $\alpha_0, \cdots, \alpha_{m-1}$ which are selected by our chain of congruences from among the m^m possible ways of selecting m elements each ranging over $0, 1, \cdots, m-1$, must be a residue system; that is, the congruences of the chain constitute also a *sufficient* condition for $\alpha_0, \cdots, \alpha_{m-1}$ to be a residue system, q.e.d.

This proof settles the desideratum of § 12, since, if the chain of congruences

should imply any more restrictions on the α than we have admitted, the number of possible residue systems would be smaller than $N(m)$.

The preceding work also proves

THEOREM XIV: *A residue system modulo m is completely determined by its first $\mu(m)$ elements (or by any $\mu(m)$ consecutive elements (see § 8, end)); but these $\mu(m)$ elements are not independent of each other; they are related in the manner explained in § 12. A complete description of these interrelations is given by the characteristic $C(m)$.*

This method of constructing the totality of residue systems for a given modulus m is unsymmetrical in that it does not deal with all elements in the same fashion. But it should be kept in mind that no one element is qualitatively distinguished above the others, since, by replacing in the corresponding polynomial x by $x - a$, any element may be brought to any other position, through a cyclic interchange. In particular, if all residue systems modulo m were written one under another,

$$\begin{array}{cccc} \alpha_0 & \alpha_1 & \cdots & \alpha_{m-1} \\ \alpha_0' & \alpha_1' & \cdots & \alpha_{m-1}' \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_0^{(N(m)-1)} & \alpha_1^{(N(m)-1)} & \cdots & \alpha_{m-1}^{(N(m)-1)}, \end{array}$$

there would be in each vertical column $N(m)/m$ zero's, $N(m)/m$ one's, $N(m)/m$ two's, etc., as is easily seen.

We insert a few simple remarks:

1. Assume $m = p_1 \cdot p_2 \cdots p_\tau$. We consider the congruences (Lemma 9, § 10)

$$\alpha_{x+p_i} \equiv \alpha_x \pmod{p_i} \qquad (i = 1, 2, \cdots, \tau).$$

By counting the number of systems $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ which satisfy these congruences, we are led again to the number $N(m)$, so that we may add to Theorem XIII:

COROLLARY: *For $m = p_1 \cdot p_2 \cdots p_\tau$, the set $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ form a residue system modulo m when and only when*

$$\alpha_k \equiv \alpha_{k+p_i} \equiv \alpha_{k+2p_i} \equiv \alpha_{k+3p_i} \equiv \cdots \pmod{p_i} \quad \begin{pmatrix} k = 0, 1, \cdots, p_i - 1 \\ i = 1, 2, \cdots, \tau \end{pmatrix}.$$

Similarly, we may make use of Definition 9, § 11, for $m = p^\nu$.

2. Assume $m = p$. In this case we have no problem. $N(p) = p^p$, and therefore every set $\alpha_0, \alpha_1, \cdots, \alpha_{p-1}$, $0 \leqq \alpha_i < p$, is the residue system of exactly one completely reduced polynomial modulo p. (See § 11 (*a*)).

In all other cases (m not a prime), we may not select the elements of our set at random from the numbers $0, 1, \cdots, m - 1$, and expect to have a

residue system modulo m of a polynomial with integral coefficients, since $N(m) < m^m$ for m not prime* (§ 6).

3. For polynomials with *fractional* (including integral) *coefficients, but which give integral values for all integral* x—we denote for the moment such polynomials by $u(x)$—the following is obvious when one makes use of arithmetical progressions:

Given any set of m integers $\beta_0, \beta_1, \cdots, \beta_{m-1}$, there always exists a polynomial $u(x)$ of degree $\leqq m$ for which $u(i) = \beta_i$.

It is therefore, a fortiori, always possible to determine a polynomial $u(x)$ which has an assigned residue system for a modulus m.

Examples.† $m = 2 \cdot 3 \cdot 5 \cdot 11$: $\mu(m) = 11$;

$$C(m) = \begin{pmatrix} 2 & 1 & 2 & 6 \\ 11 \cdot 5 \cdot 3 \cdot 2 & 11 \cdot 5 \cdot 3 & 11 \cdot 5 & 11 \end{pmatrix};$$

$N(m) = 2^2 \cdot 3^3 \cdot 5^5 \cdot 11^{11}$. For the totality of residue systems modulo $2 \cdot 3 \cdot 5 \cdot 11$ we read off from $C(m)$:

Each of the first two elements α_0, α_1 (or any two consecutive elements) may have any one of the m values $0, 1, \cdots, m-1$;

the one element α_2 may have any one of $11 \cdot 5 \cdot 3$ values which are determined from α_0, α_1 by a congruence of the chain;

each of the two elements α_3, α_4 may have any one of the $11 \cdot 5$ values which are determined from $\alpha_0, \alpha_1, \alpha_2$ by a congruence of the chain;

each of the six elements $\alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9, \alpha_{10}$ may have any one of the 11 values determined from $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ by a congruence of the chain;

each of the remaining $330 - 11 = 319$ elements $\alpha_{11}, \cdots, \alpha_{329}$ is completely determined by the first eleven, $\alpha_0, \cdots, \alpha_{10}$.

Chain of congruences: $\{11, 1\}$; $\{5, 11\}$; $\{3, 11 \cdot 5\}$; $\{2, 11 \cdot 5 \cdot 3\}$, all modulo $2 \cdot 3 \cdot 5 \cdot 11$; or (see Corollary above) $\alpha_{x+11} \equiv \alpha_x \bmod 11$; $\alpha_{x+5} \equiv \alpha_x \bmod 5$; $\alpha_{x+3} \equiv \alpha_x \bmod 3$; $\alpha_{x+2} \equiv \alpha_x \bmod 2$.

For the practical determination of the complete residue system modulo m, when a sufficient number of consecutive elements are given to uniquely characterize it, compare § 9.

Example. $m = 3^{11}$:

$$C(3^{11}) = \begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 3^{11} & 3^{10} & 3^9 & 3^7 & 3^5 & 3^5 & 3^3 & 3^2 & 3^1 \end{pmatrix};$$

$N(3^{11}) = 3^{162}$ (as compared with $(3^{11})^{3^{11}} = 3^{1946817}$ possible sets of 3^{11} elements chosen independently from $0, \cdots, 3^{11} - 1$).

The chain of congruences is (from $S(3^{11})$, see § 4) $\{27, 1\}$; $\{24, 3\}$; $\{21, 3^2\}$; $\cdots$; $\{6, 3^9\}$; $\{3, 3^{10}\}$, all modulo 3^{11}.

Each of the first three elements of a residue system modulo 3^{11} may be arbitrarily chosen from the 3^{11} numbers $0, \cdots, 3^{11} - 1$; and, similarly, each element of the jth group of three elements may have any of the t_j values determined by the $(11 - j)$th congruence of the chain (not counting the trivial congruence), where $j = 1, 2, \cdots, 9$; $t_1 = 3^{11}$, $t_2 = 3^{10}$, $t_3 = 3^9$, $t_4 = 3^7$, $t_5 = 3^5$, $t_6 = 3^5$, $t_7 = 3^3$, $t_8 = 3^2$, $t_9 = 3^1$. The remaining $3^{11} - 27$ elements are then uniquely determined.

* For example, for $m = 5$, the set $0, 3, 1, 4, 2$, chosen at random, are the residue system of $0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 3x + 0$, etc. But, modulo 4, there is no polynomial with integral coefficients of which, for example, $1, 0, 0, 2$ is the residue system.

† Compare examples in §§ 4, 6, 11.

Example. $m = 5^4 \cdot 7^3$:

$$C(5^4 \cdot 7^3) = \left(\begin{matrix} 5 \\ 5^4 \cdot 7^3 \end{matrix} \middle| \begin{matrix} 2 \\ 5^3 \cdot 7^3 \end{matrix} \middle| \begin{matrix} 3 \\ 5^3 \cdot 7^2 \end{matrix} \middle| \begin{matrix} 4 \\ 5^2 \cdot 7^2 \end{matrix} \middle| \begin{matrix} 1 \\ 5^2 \cdot 7 \end{matrix} \middle| \begin{matrix} 5 \\ 5 \cdot 7 \end{matrix} \middle| \begin{matrix} 1 \\ 7 \end{matrix} \right);$$

$N(5^4 \cdot 7^3) = 5^{50} \cdot 7^{42}$ (as compared with $5^{857500} \cdot 7^{643125}$ possible combinations).

The first five elements may be assumed chosen at random; for the next two we may still choose from $5^3 \cdot 7^3$ numbers lying between $0, 5^4 \cdot 7^3 - 1$, etc.; in the set comprising the sixteenth to twentieth elements each element may be chosen from among $5 \cdot 7$ numbers; the twenty-first element may be chosen from 7 numbers; all the others ($5^4 \cdot 7^3 - 21$ in number) are then determined.

The chain of congruences may be written, from $S(5^4 \cdot 7^3)$ (compare § 4): $1 \cdot \alpha_{x+21} \equiv l$; $7 \cdot \alpha_{x+20} \equiv l$; $5 \cdot 7 \cdot \alpha_{x+15} \equiv l$; $5^2 \cdot 7 \cdot \alpha_{x+14} \equiv l$; $5^2 \cdot 7^2 \cdot \alpha_{x+10} \equiv l$; $5^3 \cdot 7^2 \cdot \alpha_{x+7} \equiv l$; $5^3 \cdot 7^3 \cdot \alpha_{x+5} \equiv l$, all modulo $5^4 \cdot 7^3$; or, in full:

$$1 \cdot (\alpha_{x+21} - \tbinom{21}{1} \cdot \alpha_{x+20} + \tbinom{21}{2} \cdot \alpha_{x+19} - \cdots - \alpha_x) \equiv 0,$$

$$7 \cdot (\alpha_{x+20} - \tbinom{20}{1} \cdot \alpha_{x+19} + \tbinom{20}{2} \cdot \alpha_{x+18} - \cdots + \alpha_x) \equiv 0,$$

. . . . . .

$$5^3 \cdot 7^3 \cdot (\alpha_{x+5} - \tbinom{5}{1} \cdot \alpha_{x+4} + \tbinom{5}{2} \cdot \alpha_{x+3} - \cdots - \alpha_x) \equiv 0, \text{ all modulo } 5^4 \cdot 7^3.$$

As a last example, we select a number containing more than two distinct prime factors:

Example. $m = 2^7 \cdot 3^4 \cdot 7^3$: referring to § 6 for $C(2^7 \cdot 3^4 \cdot 7^3)$ and $S(2^7 \cdot 3^4 \cdot 7^3)$, we find $N(m) = 2^{40} \cdot 3^{27} \cdot 7^{21}$, and see that:

$\alpha_{0,1}$ may be assigned any values $0, \cdots, m-1$;

α_2 may be assigned any one of $2^6 \cdot 3^4 \cdot 7^3$ values;

α_3 " " " " " " $2^6 \cdot 3^3 \cdot 7^2$ " ;

$\alpha_{4,5}$ may each be assigned any of $2^4 \cdot 3^3 \cdot 7^2$ values;

α_6 may be assigned any one of $2^3 \cdot 3^2 \cdot 7^3$ values;

α_7 " " " " " " $2^3 \cdot 3^2 \cdot 7$ " ;

α_8 " " " " " " $3^2 \cdot 7$ " ;

$\alpha_{9,10,11,12,13}$ may each be assigned any of 7 values.

The remaining 508018 elements of the residue system are then uniquely determined.

In view of the results derived in §§ 8–13, we may say:

THEOREM XV: *The chain of residual congruences of the second kind, and likewise the symbols $S(m)$ and $C(m)$, are obtainable by means of simple rational operations and determine*

1. *the structure of the totality of complete residue systems modulo m of polynomials with integral coefficients;*
2. *the structure of the individual residue system modulo m of a polynomial with integral coefficients.*

IV. OUTLINE OF THE ISOMORPHISM BETWEEN POLYNOMIALS AND RESIDUE SYSTEMS

§ 14. Correspondence between completely reduced polynomials and complete residue systems.—Résumé

Our work up to the present point has established a close analogy between completely reduced polynomials on the one hand and complete residue systems

on the other hand. The following definitions serve to emphasize this correspondence.

DEFINITION 11: *A completely reduced polynomial modulo* m, $c_0 + c_1 \cdot x + \cdots + c_{\mu(m)-1} \cdot x^{\mu(m)-1}$, *is denoted by its coefficients* $(c_0, c_1, \cdots, c_{\mu(m)-1})_m$, *where the coefficients of missing terms (also of the highest powers of* x, *if missing) are denoted by* 0.

A complete residue system modulo m, $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, *is denoted by the* $\mu(m)$ *first elements* $[\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$.

We know that to each $(c_0, c_1, \cdots, c_{\mu(m)-1})_m$ corresponds one and only one $[\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$, in such manner that $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{m-1}$ form the residue system modulo m of $c_0 + c_1 x + c_2 x^2 + \cdots + c_{\mu(m)-1} \cdot x^{\mu(m)-1}$; and this polynomial is the only completely reduced polynomial modulo m to which belongs the residue system $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{m-1}$. This leads to

DEFINITION 12: *If* $[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m$ *is the residue system modulo* m *of the polynomial* $(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m$, *we write*

$$(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m \sim [\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m,$$

or

$$[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m \sim (c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m,$$

and call the residue system and the polynomial equivalent (each to the other).

If we consider for a given m the totality of the $(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m$ and the totality of the $[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m$, we see from our preceding work that the relations between the various $(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m$ and the various $[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m$ are abstractly identical. To recapitulate (with the notation used throughout):

The first $\mu(d_{\tau-1})$ coefficients $c_0, c_1, \cdots, c_{\mu(d_{\tau-1})-1}$ may be selected at random from the numbers $0, 1, \cdots, m-1$, permitting repetition; similarly the first $\mu(d_{\tau-1})$ residues $\alpha_0, \alpha_1, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ may be selected at random from the numbers $0, 1, \cdots, m-1$, permitting repetition;

and in the same manner:

any subset of $\mu(d_{i-1}) - \mu(d_i)$ coefficients $c_{\mu(d_i)}, \cdots, c_{\mu(d_{i-1})-1}$ may be selected at random from m/d_i numbers, namely from

$$0, 1, \cdots, (m/d_i) - 1 \qquad (i = 1, 2, \cdots, \tau);$$

any subset of $\mu(d_{i-1}) - \mu(d_i)$ residues $\alpha_{\mu(d_i)}, \cdots, \alpha_{(d_{i-1})-1}$ may be selected at random from m/d_i numbers, namely from the numbers of the set $0, 1, \cdots, m$ determined by the congruence $\alpha_{x+\mu(d_i)} \equiv l \bmod d_i$.

This isomorphism holds true to the last set of $\mu(m) - \mu(d_1)$ coefficients $c_{\mu(d_1)}, \cdots, c_{\mu(m)-1}$ and the set of $\mu(m) - \mu(d_1)$ elements of the residue system $\alpha_{\mu(d_1)}, \cdots, \alpha_{\mu(m)-1}$. All coefficients of the completely reduced polynomial are thereby determined, while the residue system is also determined

because the $m - \mu(m)$ elements $\alpha_{\mu(m)}, \cdots, \alpha_{m-1}$ which are not represented in the symbol $[\alpha_0, \cdots, \alpha_{\mu(m)-1}]_m$ are uniquely determined by $\alpha_0, \cdots, \alpha_{\mu(m)-1}$.

RÉSUMÉ

MODULUS m

POLYNOMIALS	RESIDUE SYSTEMS
Residual congruence: § 2	*Residual congruence (second kind):* § 10
For every divisor d of m exists a congruence:	
$\frac{m}{d} \cdot \Pi_{k=0}^{\mu(d)-1}(x-k) \equiv 0 \pmod m$,	$\frac{m}{d} \cdot \sum_{i=0}^{\mu(d)} \binom{\mu(d)}{i} \cdot \alpha_{x+\mu(d)-i} \equiv 0 \pmod m$,
or	or
$\frac{m}{d} \cdot x^{\mu(d)} \equiv \psi(x) \pmod m$	$\frac{m}{d} \cdot \alpha_{x+\mu(d)} \equiv l \pmod m$
or	or
$\left\{\mu(d), \frac{m}{d}\right\}_m$.	$\left\}\mu(d), \frac{m}{d}\right\{_m$.
Signature of m: § 4	*Signature of m (second kind):* § 11
$S(m) = \begin{pmatrix} \mu(m) & \cdots & \mu(d_i) & \cdots & \mu(d_\tau) \\ 1 & \cdots & m/d_i & \cdots & m/d_\tau \end{pmatrix}$.	$S(m) = \begin{pmatrix} \mu(m) & \cdots & \mu(d_i) & \cdots & \mu(d_\tau) \\ 1 & \cdots & m/d_i & \cdots & m/d_\tau \end{pmatrix}$.
Chain of residual congruences: § 3	*Chain of residual congruences (second kind):* § 11
$\frac{m}{d_i} \cdot x^{\mu(d_i)} \equiv \psi(x) \pmod m$;	$\frac{m}{d_i} \cdot \alpha_{x+\mu(d_i)} \equiv l \pmod m$;
or	or
$\left\{\mu(d_i), \frac{m}{d_i}\right\}_m$ $(i=0, 1, 2, \cdots, \tau)$.	$\left\}\mu(d_i), \frac{m}{d_i}\right\{_m$ $(i=0, 1, 2, \cdots, \tau)$.
Characteristic of m: § 5	*Characteristic of m (second kind):* § 12
$C(m) = \begin{pmatrix} \mu(d_{\tau-1}) & \mu(d_{\tau-2})-\mu(d_{\tau-1}) & \cdots & \mu(d_{i-1})-\mu(d_i) & \cdots & \mu(m)-\mu(d_1) \\ m & \frac{m}{d_{\tau-1}} & & \frac{m}{d_i} & & \frac{m}{d_1} \end{pmatrix} = C(m)$.	
Completely reduced polynomial: §§ 5, 14	*Complete residue system:* §§ 12, 14
$c_0 + c_1 \cdot x + \cdots + c_{\mu(m)-1} \cdot x^{\mu(m)-1}$	$\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}, \alpha_{\mu(m)}, \cdots, \alpha_{m-1}$
$= (c_0, c_1, \cdots, c_{\mu(m)-1})_m$	$= [\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$
$(c_0, c_1, \cdots, c_{\mu(m)-1})_m \sim$	$[\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$
Number of completely reduced polynomials: § 6	*Number of complete residue systems:* § 13
$N(m)$.	$N(m)$.

UNIVERSITY OF ILLINOIS,
URBANA, ILLINOIS

ON CERTAIN TWO-POINT PROPERTIES OF GENERAL FAMILIES OF CURVES*

BY

JESSE DOUGLAS

In a paper published in 1903,† R. Straubel proved an important theorem of geometrical optics to the following effect. In any isotropic medium,—in which the index of refraction is therefore a function of position only, $\nu(x, y, z)$,—let a and b be any two points. Imagine an element of area $\delta\sigma_1$ to be placed at b normal to the (curvilinear) ray ab, and let it subtend at a the solid angle $\delta\omega_1$. Reversing the situation, suppose an element $\delta\sigma_2$ placed likewise at a to subtend at b the solid angle $\delta\omega_2$. Then the relation

$$\frac{\delta\sigma_1}{\delta\omega_1} : \nu^2(a) = \frac{\delta\sigma_2}{\delta\omega_2} : \nu^2(b)$$

will subsist. In n dimensions ν^{n-1} takes the place of ν^2.

Straubel's theorem was made the subject of a paper by T. Levi-Civita,‡ who generalized it to the case of a non-isotropic medium. Levi-Civita's fundamental result is as follows. Consider the geodesics of a general (curved) n-dimensional variety V_n. Denoting by a and b any two points in V_n, let an $(n-1)$-dimensional element of extent $\delta\sigma_1$ placed at b normal to the geodesic ab subtend at a the solid angle $\delta\omega_1$. If then an element $\delta\sigma_2$ placed likewise at a subtends at b the solid angle $\delta\omega_2$, we shall have

$$\frac{\delta\sigma_1}{\delta\omega_1} = \frac{\delta\sigma_2}{\delta\omega_2}.$$

The object of the present paper is to develop general geometric theorems in the above order of ideas for an arbitrary family of curves. In particular, the property of Levi-Civita's theorem is shown to hold for a wider class

* Presented to the Society, April, 1917. See Bulletin of the American Mathematical Society, vol. 23 (1916–17), p. 441.

† *Ueber einen allgemeinen Satz der geometrischen Optik und einige Anwendungen*, Physikalische Zeitschrift, vol. 4 (1903), pp. 114–117.

‡ *Una proprièta de simmetria delle traiettorie dinamiche spiccati da due punti*, Atti della Reale Accademia dei Lincei, vol. 24, April, 1915. The notation is different from that of the present paper.

of curve families than the geodesics. Straubel's theorem is discussed as to its purely geometrical implications; it is shown, among other things, that the Straubel relation is not characteristic of the curve families that can arise as the totality of paths of light in an isotropic medium,—that is, of the natural families, so called.*

The method of investigation is characterized by the systematic use of the fact that, given a family of curves defined by any system of differential equations, the curves infinitesimally near to a given one obey a system of linear differential equations—the equations of variation (Poincaré) or auxiliary equations (Darboux) of those that define the given curve family.

I. Theory for two dimensions

1. **Definitions. The functions $V(a,b)$ and $W(a,b)$.** Consider any family of ∞^2 curves in the plane, as defined by a differential equation of the second order, $y'' = F(x, y, y')$.

Let a and b be any two points of the plane. Then, under suitable restrictions,† there is a unique curve C of the given family joining a and b. Imagine an infinitesimal element bb' of length $\delta\sigma_1$ to be placed at b normal to C, and let C_1 be the curve of the given family that joins b' to a. Denoting by $\delta\omega_1$ the infinitesimal angle enclosed at a between C_1 and C, the ratio $\delta\sigma_1/\delta\omega_1$ is a function of the two points a and b; we call it $V(a,b)$.

Similarly, let the element aa' of length $\delta\sigma_2$ be normal to C at a, and let C_2 denote the curve that passes through a' and b. Then designating as $\delta\omega_2$ the angle at b between C_2 and C, the ratio $\delta\sigma_2/\delta\omega_2$ is appropriately $V(b,a)$. It is to be remarked that in general $V(a,b) \neq V(b,a)$.

Besides the defining equations

$$V(a,b) = \frac{\delta\sigma_1}{\delta\omega_1}, \qquad V(b,a) = \frac{\delta\sigma_2}{\delta\omega_2},$$

we introduce also the notation

$$W(a,b) = \frac{V(a,b)}{V(b,a)}.$$

Our specific object is the study of the geometric functions $V(a,b)$, $W(a,b)$.

2. **Expression for $V(a,b)$.** We have under consideration a doubly-infinite system of curves, defined by a differential equation of the second order,

$$Y'' = F(X, Y, Y'). \tag{1}$$

To every set of initial values x, y, p for X, Y, Y' there corresponds a

*After E. Kasner, *Differential-geometric aspects of dynamics*, Princeton Colloquium Lectures (1912), pp. 34–72, or his papers in these Transactions, vol. 10 (1909), p. 72, and vol. 11 (1910), p. 121, where several sets of completely characteristic properties of natural families are given.

† See Picard, *Traité d'Analyse*, vol. 3, pp. 90–99.

definite curve; let its equation be

$$Y = Y(X;\, x, y, p). \tag{2}$$

Explicitly, we may write Y as a power series; the first terms are

$$Y = y + p(X - x) + \tfrac{1}{2} F(x, y, p)(X - x)^2 + \cdots. \tag{2'}$$

Let the coördinates of a be (x_1, y_1), those of b, (x_2, y_2); let the slope of the curve C be p_1 at a, and p_2 at b. Then in (2), C corresponds to the initial values x_1, y_1, p_1; also to the initial values x_2, y_2, p_2. Suppose that for these values (2) reduces to

$$Y = y(X), \tag{3}$$

which is then the equation of C.

The curve C_1 will correspond to

$$x = x_1, \qquad y = y_1, \qquad p = p_1 + \delta p_1,$$

denoting by the last the slope of C_1 at a; the equation of C_1 will be therefore

$$Y = y(X) + \delta p_1\, Y_p(X;\, x_1, y_1, p_1),$$

where the powers of δp_1 beyond the first have been neglected as infinitesimals of higher order. The subscript p denotes partial differentiation with respect to that variable.

Since x_1, y_1, p_1 are fixed, Y_p is a function of X alone; we introduce for it the notation

$$\eta_1(X) = Y_p(X;\, x_1, y_1, p_1),$$

and write the equation of C_1 in the form

$$Y = y(X) + \delta p_1\, \eta_1(X). \tag{4$_1$}$$

In the same way, the equation of C_2 will be

$$Y = y(X) + \delta p_2\, \eta_2(X), \tag{4$_2$}$$

where

$$\eta_2(X) = Y_p(X;\, x_2, y_2, p_2).$$

In the figure of the preceding section let bb'' denote the element of length at b parallel to the y-axis and included between the curves C and C_1. Obviously,

$$bb'' = \delta p_1\, \eta_1(x_2).$$

Hence

$$\delta\sigma_1 = bb'' \cos \sphericalangle\, b'\, bb'' = \frac{\delta p_1\, \eta_1(x_2)}{(1 + p_2^2)^{1/2}}.$$

Also

$$\delta\omega_1 = \delta \tan^{-1} p_1 = \frac{\delta p_1}{1 + p_1^2}.$$

Therefore

$$(5_1) \qquad V(a,b) = \frac{\delta\sigma_1}{\delta\omega_1} = \frac{1+p_1^2}{(1+p_2^2)^{1/2}}\eta_1(x_2).$$

To obtain the formula for $V(b,a)$, we have only to interchange systematically the rôles of a and b. The result is

$$(5_2) \qquad V(b,a) = \frac{\delta\sigma_2}{\delta\omega_2} = -\frac{1+p_2^2}{(1+p_1^2)^{1/2}}\eta_2(x_1),$$

where the significance of the minus sign is as follows: in forming $V(a,b)$ the curve C is viewed in the sense ab; in forming $V(b,a)$, in the reverse sense ba.

3. **Expression for $W(a,b)$.** The important fact concerning $\eta_1(X)$ and $\eta_2(X)$ is that they are two independent solutions of a certain linear differential equation of the second order.* To see this, return to the equations (1) and (2) of the preceding section. (2) represents the general solution of (1); this means that we have identically in the four variables X, x, y, p:

$$Y''(X;\, x, y, p) = F[X,\, Y(X;\, x, y, p),\; Y'(X;\, x, y, p)],$$

where the accents denote partial differentiation with respect to X. We may differentiate this identity with respect to p, obtaining:

$$(Y'')_p = F_y(Y_p) + F_{y'}(Y')_p.\dagger$$

Under the assumption that all the derivatives involved are continuous, the differentiations with respect to X and p are commutative; the above equation may therefore be rewritten:

$$(Y_p)'' = F_y(Y_p) + F_{y'}(Y_p)'.$$

When x, y, p are set equal respectively to x_1, y_1, p_1, Y_p reduces to $\eta_1(X)$; when the same letters are equal to x_2, y_2, p_2, Y_p reduces to $\eta_2(X)$. It follows that $\eta_1(X)$ and $\eta_2(X)$ obey the differential equation

$$(6) \qquad \eta''(X) = F_{y'}\,\eta'(X) + F_y\,\eta(X),$$

where it is understood that in $F_{y'}(X, Y, Y')$, $F_y(X, Y, Y')$ we are to substitute for Y and Y' from the curve C:

$$Y = y(X), \qquad Y' = y'(X),$$

so that these coefficients are functions of X alone, where X represents the abscissa along C.

The functions η_1, η_2 will be completely defined by giving their values and those of their first derivatives for an initial value of X. These are determined as follows. Differentiating (2′) with respect to p, we have, after writing x,

* The equation of variation of the differential equation (1).

† For convenience of notation, small letters are used instead of capitals in denoting the partial derivatives of the function F.

y, p equal to x_1, y_1, p_1:

$$\eta_1(X) = (X - x_1) + \tfrac{1}{2} F_p(x_1, y_1, p_1)(X - x_1)^2 + \cdots,$$

hence

$$(7_1) \qquad \eta_1(x_1) = 0, \qquad \eta_1'(x_1) = 1.$$

Similarly we find

$$(7_2) \qquad \eta_2(x_2) = 0, \qquad \eta_2'(x_2) = 1.$$

Now $\eta_1(X)$, $\eta_2(X)$, as two independent solutions of the linear differential equation (6), must obey the relation

$$\begin{vmatrix} \eta_1(X) & \eta_2(X) \\ \eta_1'(X) & \eta_2'(X) \end{vmatrix} = e^{\int_k^X F_{y'}\, dX},$$

where k is an undetermined constant.

In this write successively

$$X = x_1, \qquad X = x_2,$$

and take account of the equations (7_1), (7_2); there results:

$$-\eta_2(x_1) = e^{\int_k^{x_1} F_{y'}\, dx},$$

$$\eta_1(x_2) = e^{\int_k^{x_2} F_{y'}\, dx}.$$

Dividing the second equation by the first, the unknown k is eliminated:

$$(8) \qquad -\frac{\eta_1(x_2)}{\eta_2(x_1)} = e^{\int_{x_1}^{x_2} F_{y'}\, dx}.$$

The result thus obtained applies directly to the derivation of an expression for $W(a, b)$. By definition,

$$W(a, b) = \frac{V(a, b)}{V(b, a)};$$

so that, substituting the expressions (5_1), (5_2) for $V(a, b)$, $V(b, a)$, we have

$$W(a, b) = -\frac{(1 + p_1^2)^{3/2}}{(1 + p_2^2)^{3/2}} \frac{\eta_1(x_2)}{\eta_2(x_1)}.$$

Hence, by equation (8),

$$W(a, b) = \frac{(1 + p_1^2)^{3/2}}{(1 + p_2^2)^{3/2}} e^{\int_{x_1}^{x_2} F_{y'}\, dx}.$$

This can easily be transformed into

$$(9) \qquad W(a, b) = e^{\int_{x_1}^{x_2} \left(F_{y'} - \frac{3y'F}{1 + y'^2} \right) dx}.$$

The function $W(a, b)$ is an intrinsic geometric quantity, being, that is to say, independent of the selection of coördinate axes. It is desirable to find for it an expression in which only intrinsic elements shall figure.

This is attained through the following considerations. We are dealing with a family of ∞^2 curves of which one passes through every point in every direction. Let $\partial\gamma/\partial\theta$ denote the rate of change of curvature with respect to variation of direction as, remaining at any fixed point, we pass from curve to curve of the family. The expression for $\partial\gamma/\partial\theta$ is

$$\frac{\partial\gamma}{\partial\theta} = \frac{(1+y'^2)F_{y'} - 3y'F}{(1+y'^2)^{3/2}};$$

and to pass from this to the integrand of (9), we have only to introduce the element of arc along C,

$$ds = (1+y'^2)^{1/2}\,dx.$$

Multiplying, we get

$$\frac{\partial\gamma}{\partial\theta}\,ds = \left(F_{y'} - \frac{3y'F}{1+y'^2}\right)dx;$$

therefore, according to (9),

$$W(a,b) = e^{\int_a^b \frac{\partial\gamma}{\partial\theta}\,ds}. \tag{10}$$

The path of integration is the arc ab of the curve C.

4. **The multiplicative property of** $W(a,b)$. From the result (10) certain simple corollaries follow directly.

Consider any three points a, b, c located not in general position but on the same curve C of the double infinite family under consideration. We have

$$W(a,b) = e^{\int_a^b \frac{\partial\gamma}{\partial\theta}\,ds}, \qquad W(b,c) = e^{\int_b^c \frac{\partial\gamma}{\partial\theta}\,ds}, \qquad W(a,c) = e^{\int_a^c \frac{\partial\gamma}{\partial\theta}\,ds}.$$

Multiplying together the first two of these equations and taking account of the additive nature of integration, we find

$$W(a,b)\cdot W(b,c) = W(a,c). \tag{11}$$

Along any individual curve C the function $W(a,b)$ is of multiplicative character.

5. **Transitivity of the relation** $V(a,b) = V(b,a)$. A second result follows as a sub-corollary of (11). We have remarked that in general $V(a,b) \neq V(b,a)$. But suppose, as a special situation, that a, b, c are three points *on the same curve* C, and that

$$V(a,b) = V(b,a), \qquad \text{and} \qquad V(b,c) = V(c,b).$$

Then it must follow as a consequence that

$$V(a,c) = V(c,a);$$

for the above relations are equivalent to

$$W(a,b) = 1, \qquad W(b,c) = 1,$$

from which by (11) it follows that

$$W(a, c) = 1,$$

or that

$$V(a, c) = V(c, a).$$

Thus, along any individual curve C, the relation $V(a, b) = V(b, a)$ is a transitive one. We remark that this fact is not at all evident from the geometric definition of $V(a, b)$.

6. **Curve families with symmetric $V(a, b)$.** The particular doubly infinite systems of curves for which $V(a, b)$ is a symmetric function of the two points a and b are found immediately from a consideration of (10). We wish to have

$$V(a, b) \equiv V(b, a),$$

which is equivalent to

$$W(a, b) \equiv 1,$$

or again, equivalent to

$$\int_a^b \frac{\partial \gamma}{\partial \theta} ds = 0,$$

for any two points a and b. For this, the integrand $\partial\gamma/\partial\theta$ must be identically zero. Recalling the meaning of $\partial\gamma/\partial\theta$, we have therefore the

THEOREM. *The necessary and sufficient condition that, for a family of ∞^2 curves in the plane, the corresponding two-point function, $V(a, b)$, be symmetric, is that at any given point the curvature be the same for all the curves of the family through that point.*

This means that γ may be a function of x,y, but not of y'. Curve families with symmetric $V(a, b)$ are therefore characterized by differential equations of the form

$$y'' = (1 + y'^2)^{3/2} G(x, y). \tag{12}$$

7. **Straubel's theorem. Geometric interpretation.** The theorem of Straubel stated at the beginning of this paper follows from applying the formula for $W(a, b)$ to the case of a family of light rays.

Imagine in the plane an isotropic optical medium, in which the index of refraction is $\nu(x, y)$. Such a medium gives rise to a system of ∞^2 curves as paths of light, these being determined as the extremals of the calculus of variations problem

$$\int \nu(x, y)\, ds = \text{min.},$$

or by the equivalent Euler-Lagrange differential equations:

$$y'' = (L_y - y' L_x)(1 + y'^2) \tag{13}$$

where $L = \log \nu$. Following E. Kasner,* we shall term a family of curves of the type (13) a natural family.

*Princeton Colloquium Lectures, pp. 34–37.

In applying the formula (9) to natural families, we have

$$F_{y'} - \frac{3y'F}{1+y'^2} = -L_x - y'L_y = -\frac{d}{dx}L(x,y),$$

therefore

$$W(a,b) = \frac{e^{L(x_1,y_1)}}{e^{L(x_2,y_2)}} = \frac{\nu(x_1,y_1)}{\nu(x_2,y_2)},$$

that is

$$\frac{V(a,b)}{V(b,a)} = \frac{\nu(a)}{\nu(b)}, \tag{14}$$

which is Straubel's result.

Straubel's theorem is not purely geometric in so far as it contains the indices of refraction $\nu(a)$, $\nu(b)$. An exclusively geometric form is obtainable by considering any three points a, b, c of the plane. We shall have

$$W(a,b) = \frac{\nu(a)}{\nu(b)}, \qquad W(b,c) = \frac{\nu(b)}{\nu(c)}, \qquad W(a,c) = \frac{\nu(a)}{\nu(c)},$$

from which equations the indices of refraction can be eliminated, giving

$$W(a,b) \cdot W(b,c) = W(a,c).$$

Therefore:

The multiplicative relation (11) *which holds in the case of any doubly infinite family of curves when* a, b, c *are on the same curve, holds in the case of a natural family for general position of* a, b, c.

This is the purely geometric content of Straubel's theorem.

8. **Converse of Straubel's theorem.** Is the Straubel property characteristic of natural families? For the answer we return to (14). When can we define a function $\nu(x,y)$ of the points of the plane and have for any two points a and b:

$$\frac{V(a,b)}{V(b,a)} = \frac{\nu(a)}{\nu(b)}\,?$$

By (9), the condition in question is equivalent to

$$\int_{x_1}^{x_2}\left(F_{y'} - \frac{3y'F}{1+y'^2}\right)dx = \log\nu(x_1,y_1) - \log\nu(x_2,y_2) = -L(x,y)\Big|_{x_1,y_1}^{x_2,y_2}.$$

For this relation the necessary and sufficient condition is

$$F_{y'} - \frac{3y'F}{1+y'^2} = -\frac{d}{dx}L(x,y) = -L_x - y'L_y.$$

The last is to be regarded as a partial differential equation for F. It can be integrated by means of the integrating factor $1/(1+y'^2)^{\frac{3}{2}}$, using which, we find

$$\frac{F}{(1+y'^2)^{\frac{3}{2}}} = \frac{L_y - y'L_x}{(1+y'^2)^{\frac{1}{2}}} + G(x,y),$$

where $G(x, y)$ is the constant of integration (with respect to y'). Thus we obtain for F the expression

$$F = (L_y - y' L_x)(1 + y'^2) + G(x, y)(1 + y'^2)^{\frac{3}{2}}, \tag{15}$$

and have the theorem:

The Straubel property is not characteristic of natural families—it holds for the more general type defined by (15).*

9. **Theory for an arbitrary surface.** In extending the theory of the functions V and W to a family of ∞^2 curves upon a general surface, no new difficulties present themselves apart from the increased length of calculation. The typical feature is that the geodesic curvature γ_g replaces the γ of the plane.

The main result arrived at is the formula for $W(a, b)$:

$$W(a, b) = e^{\int_a^b \frac{\partial \gamma_g}{\partial \theta} ds}.$$

We consider particularly the special systems of ∞^2 curves for which $V(a, b) \equiv V(b, a)$. Evidently, these are the ones for which $\partial \gamma_g / \partial \theta \equiv 0$, hence the

THEOREM. *The necessary and sufficient condition that a family of ∞^2 curves upon an arbitrary surface have the property $V(a, b) \equiv V(b, a)$ is that the geodesic curvature be the same at any given point for all the curves through that point.*

Such families are characterized by equations of the form $\gamma_g = G(x, y)$, x and y being any curvilinear coördinates upon the surface. The most interesting particular case occurs when $G(x, y)$ is identically zero, which condition defines the geodesics of the surface. The geodesics of any surface have therefore the property $V(a, b) \equiv V(b, a)$. This is the content (for $n = 2$) of the theorem of Levi-Civita enunciated at the beginning of this paper. Levi-Civita's result thus enters as a special case under the theorem stated above.

II. THEORY FOR ORDINARY THREE-DIMENSIONAL SPACE

10. **Generalities; definitions.** In extending the preceding considerations to space, we have to consider a family of curves defined by two differential equations of the second order:

$$\begin{aligned} Y'' &= F(X, Y, Z, Y', Z') \\ Z'' &= G(X, Y, Z, Y', Z'). \end{aligned} \tag{1}$$

Such a family consists of ∞^4 curves, one for each initial point and direction

* The geometric properties of curve systems of the type (15) have been studied by K. Ogura, *On the integral curves of ordinary differential equations of the second order of a certain type*, Tohoku Mathematical Journal, vol. 8 (1915), pp. 93–107.

x, y, z, p, q. Let the equations of the curve corresponding to these initial values be

$$(2) \qquad \begin{aligned} Y &= Y(X; x, y, z, p, q) \\ Z &= Z(X; x, y, z, p, q), \end{aligned}$$

so that (2) represents the general solution of (1). We can write the equations (2) explicitly as power series; the first terms are

$$(2') \qquad \begin{aligned} Y &= y + p(X - x) + \tfrac{1}{2} F(x, y, z, p, q)\,(X - x)^2 + \cdots \\ Z &= z + q(X - x) + \tfrac{1}{2} G(x, y, z, p, q)\,(X - x)^2 + \cdots . \end{aligned}$$

If we select any two points of space a and b, there will be, under the proper restrictions,* a unique curve C of the family (1) passing through these points. Let an element of area $\delta\sigma_1$ be situated at b normal to C; the curves that join the boundary of $\delta\sigma_1$ to a form at a a curvilinear cone of infinitesimal solid angle $\delta\omega_1$. Then we define:

$$V(a, b) = \frac{\delta\sigma_1}{\delta\omega_1}.$$

A similar definition determines $V(b, a)$, and as in the theory for the plane we introduce also the function

$$W(a, b) = \frac{V(a, b)}{V(b, a)}.$$

In order to derive formulas for V and W we refer the neighborhood of a to a rectangular axis system ξ, η, ζ of which the ζ-axis is the tangent to C at a. Similarly, the neighborhood of b is referred to an axis system u, v, w where w is the tangent to C at b.† We designate the plane ξ, η as π_1, the plane u, v as π_2.

The curves of the given family as they stream away from a and impinge upon the plane π_2 set up a correspondence between the directions through a and the points of π_2,—a correspondence which for directions infinitely near to ζ and therefore for points infinitely near to b is linear (affine). Now $V(a, b)$ is equal to the determinant of this linear correspondence. For $V(a, b)$ may be interpreted as the ratio of two areas correlated with one another affinely, and under an affine transformation all areas are multiplied by the determinant.

11. **The functions $\eta(X)$, $\zeta(X)$ and their linear differential equations.** Let the Cartesian coördinates of a and b be respectively (x_1, y_1, z_1), (x_2, y_2, z_2). Suppose the equations of C to be

$$(3) \qquad Y = y(X), \qquad Z = z(X);$$

* See Picard, *Traité d'Analyse*, vol. 3, pp. 90–99.

† In the choice of each axis system there is, of course, one degree of freedom, but this circumstance is indifferent for what follows.

then the direction of C at a is defined by the parameters

$$p_1 = y'(x_1), \qquad q_1 = z'(x_1),$$

and at b by the parameters

$$p_2 = y'(x_2), \qquad q_2 = z'(x_2).$$

The equations (3) of C will result upon the substitution of x_1, y_1, z_1, p_1, q_1 for x, y, z, p, q in the equations (2); also upon the substitution of x_2, y_2, z_2, p_2, q_2 for the same letters.

Let C_1 be a curve, of the family under consideration, passing through a in a direction $p_1 + \delta p_1, q_1 + \delta q_1$ infinitely near to that of C. The equations of C_1 result by writing in (2):

$$x = x_1, \qquad y = y_1, \qquad z = z_1, \qquad p = p_1 + \delta p_1, \qquad q = q_1 + \delta q_1.$$

When we then expand according to powers of $\delta p_1, \delta q_1$ we may omit the powers beyond the first as negligible in the limit, and find for the equations of C_1:

$$(3_1) \qquad \begin{aligned} Y &= y(X) + \delta p_1\, \eta_1(X) + \delta q_1\, \eta_2(X) \\ Z &= z(X) + \delta p_1\, \zeta_1(X) + \delta q_1\, \zeta_2(X), \end{aligned}$$

where we have written

$$(4_1) \qquad \begin{aligned} \eta_1(X) &= Y_p(X;\, x_1, y_1, z_1, p_1, q_1) \\ \zeta_1(X) &= Z_p(X;\, x_1, y_1, z_1, p_1, q_1), \end{aligned}$$

$$(4_2) \qquad \begin{aligned} \eta_2(X) &= Y_q(X;\, x_1, y_1, z_1, p_1, q_1) \\ \zeta_2(X) &= Z_q(X;\, x_1, y_1, z_1, p_1, q_1). \end{aligned}$$

In the same way the equations of the curve C_2 passing through b in a direction $p_2 + \delta p_2, q_2 + \delta q_2$ will be

$$(3_2) \qquad \begin{aligned} Y &= y(X) + \delta p_2\, \eta_3(X) + \delta q_2\, \eta_4(X) \\ Z &= z(X) + \delta p_2\, \zeta_3(X) + \delta q_2\, \zeta_4(X), \end{aligned}$$

where

$$(4_3) \qquad \begin{aligned} \eta_3(X) &= Y_p(X;\, x_2, y_2, z_2, p_2, q_2) \\ \zeta_3(X) &= Z_p(X;\, x_2, y_2, z_2, p_2, q_2), \end{aligned}$$

$$(4_4) \qquad \begin{aligned} \eta_4(X) &= Y_q(X;\, x_2, y_2, z_2, p_2, q_2) \\ \zeta_4(X) &= Z_q(X;\, x_2, y_2, z_2, p_2, q_2). \end{aligned}$$

The four systems η, ζ just defined are independent solutions of a certain system of two linear differential equations of the second order.* For since (2) represents the solution of the equations (1), there will result upon substitution

* The equations of variation of the differential equations (1).

of (2) in (1) two identities in X, x, y, z, p, q. Differentiating these identities with respect to p, we obtain:

$$(Y'')_p = F_y Y_p + F_z Z_p + F_{y'}(Y')_p + F_{z'}(Z')_p$$
$$(Z'')_p = G_y Y_p + G_z Z_p + G_{y'}(Z')_p + G_{z'}(Z')_p.^*$$

Assuming the derivatives involved to be continuous, the differentiations with respect to X and p are commutative, and the above equations may be rewritten:

$$(Y_p)'' = F_y(Y_p) + F_z(Z_p) + F_{y'}(Y_p)' + F_{z'}(Z_p)'$$
$$(Z_p)'' = G_y(Y_p) + G_z(Z_p) + G_{y'}(Y_p)' + G_{z'}(Z_p)'.$$

For x, y, z, p, q equal to x_1, y_1, z_1, p_1, q_1, Y_p, Z_p reduce to $\eta_1(X), \zeta_1(X)$. It follows that η_1, ζ_1 obey the linear differential equations

$$\begin{aligned} \eta''(X) &= F_{y'}\eta'(X) + F_{z'}\zeta'(X) + F_y\eta(X) + F_z\zeta(X) \\ \zeta''(X) &= G_{y'}\eta'(X) + G_{z'}\zeta'(X) + G_y\eta(X) + G_z\zeta(X), \end{aligned} \tag{5}$$

where it is understood that, in the coefficients $F_{y'}(X, Y, Z, Y', Z')$, etc., the substitutions

$$Y = y(X), \qquad Z = z(X), \qquad Y' = y'(X), \qquad Z' = z'(X)$$

are to be made, so that these coefficients are functions only of X, the abscissa along C.

In similar manner the other systems η, ζ can be shown to obey the equations (5). Each η, ζ is therefore determined if initial values are given for $\eta, \zeta, \eta', \zeta'$. For η_1, ζ_1 such values are found by differentiating (2′) with respect to p, and then replacing x, y, z, p, q by x_1, y_1, z_1, p_1, q_1; this gives:

$$\eta_1(X) = (X - x_1) + \tfrac{1}{2} F_p(x_1, y_1, z_1, p_1, q_1,)\,(X - x_1)^2 + \cdots$$
$$\zeta_1(X) = \tfrac{1}{2} G_p(x_1, y_1, z_1, p_1, q_1,)\,(X - x_1)^2 + \cdots;$$

hence

$$(6_1) \quad \eta_1(x_1) = 0, \quad \zeta_1(x_1) = 0, \quad \eta_1'(x_1) = 1, \quad \zeta_1'(x_1) = 0.$$

Similarly we find

$$(6_2) \quad \eta_2(x_1) = 0, \quad \zeta_2(x_1) = 0, \quad \eta_2'(x_1) = 0, \quad \zeta_2'(x_1) = 1,$$
$$(6_3) \quad \eta_3(x_2) = 0, \quad \zeta_3(x_2) = 0, \quad \eta_3'(x_2) = 1, \quad \zeta_3'(x_2) = 0,$$
$$(6_4) \quad \eta_4(x_2) = 0, \quad \zeta_4(x_2) = 0, \quad \eta_4'(x_2) = 0, \quad \zeta_4'(x_2) = 1.$$

The fact important for the present developments is that the four systems η, ζ, as a fundamental system of independent solutions of the equations (5),

* For convenience of notation, small letters are used instead of capitals in denoting the partial derivatives of the functions F and G.

must obey the relation

$$(7)\qquad \begin{vmatrix} \eta_1(X) & \eta_2(X) & \eta_3(X) & \eta_4(X) \\ \zeta_1(X) & \zeta_2(X) & \zeta_3(X) & \zeta_4(X) \\ \eta_1'(X) & \eta_2'(X) & \eta_3'(X) & \eta_4'(X) \\ \zeta_1'(X) & \zeta_2'(X) & \zeta_3'(X) & \zeta_4'(X) \end{vmatrix} = e^{\int_k^X (F_{y'} + G_{z'})\, dX},$$

where k is an undetermined constant. In (7), put $X = x_1$; then by reference to (6_1), (6_2),

$$(8_1)\qquad \begin{vmatrix} \eta_3(x_1) & \eta_4(x_1) \\ \zeta_3(x_1) & \zeta_4(x_1) \end{vmatrix} = e^{\int_k^{x_1} (F_{y'} + G_{z'})\, dx}.$$

Similarly, by putting $X = x_2$ and referring to (6_3), (6_4), we have

$$(8_2)\qquad \begin{vmatrix} \eta_1(x_2) & \eta_2(x_2) \\ \zeta_1(x_2) & \zeta_2(x_2) \end{vmatrix} = e^{\int_k^{x_2} (F_{y'} + G_{z'})\, dx}.$$

On dividing (8_1) into (8_2), k is eliminated; we find

$$(9)\qquad \frac{\begin{vmatrix} \eta_1(x_2) & \eta_2(x_2) \\ \zeta_1(x_2) & \zeta_2(x_2) \end{vmatrix}}{\begin{vmatrix} \eta_3(x_1) & \eta_4(x_1) \\ \zeta_3(x_1) & \zeta_4(x_1) \end{vmatrix}} = e^{\int_{x_1}^{x_2} (F_{y'} + G_{z'})\, dx}.$$

This result will be directly useful in deriving an expression for $W(a, b)$.

12. **Expression for $V(a, b)$.** Recurring to § 10, we next deduce an expression for the linear correspondence there described.

The curve C_1 which passes through a in the direction $p_1 + \delta p_1$, $q_1 + \delta q_1$ will pierce the plane π_2 in a point b_1 of coördinates $x_2 + \delta x_2$, $y_2 + \delta y_2$, $z_2 + \delta z_2$. These coördinates must satisfy the equations (3_1) of C_1; therefore

$$y_2 + \delta y_2 = y(x_2 + \delta x_2) + \delta p_1\, \eta_1(x_2 + \delta x_2) + \delta q_1\, \eta_2(x_2 + \delta x_2),$$

$$z_2 + \delta z_2 = z(x_2 + \delta x_2) + \delta p_1\, \zeta_1(x_2 + \delta x_2) + \delta q_1\, \zeta_2(x_2 + \delta x_2),$$

whence, omitting infinitesimals of higher order than the first,

$$(10)\qquad \begin{aligned} \delta y_2 &= p_2\, \delta x_2 + \delta p_1\, \eta_1(x_2) + \delta q_1\, \eta_2(x_2) \\ \delta z_2 &= q_2\, \delta x_2 + \delta p_1\, \zeta_1(x_2) + \delta q_1\, \zeta_2(x_2). \end{aligned}$$

Let the direction cosines of the u, v axes at b be

$$u:\ a,\ b,\ c$$

$$v:\ l,\ m,\ n;$$

those of the w-axis are

$$w:\ \frac{1}{\sqrt{1 + p_2^2 + q_2^2}},\ \frac{p_2}{\sqrt{1 + p_2^2 + q_2^2}},\ \frac{q_2}{\sqrt{1 + p_2^2 + q_2^2}}.$$

Since u, v, w are a trirectangular system, we have the relations

$$\begin{aligned} a + p_2 b + q_2 c &= 0 \\ l + p_2 m + q_2 n &= 0 \\ bn - cm &= \frac{1}{\sqrt{1 + p_2^2 + q_2^2}}. \end{aligned} \tag{11}$$

At the same time we may turn our attention to the ξ, η, ζ system at a, where, writing for the direction cosines

$$\text{of } \xi\text{: } \alpha,\ \beta,\ \gamma,$$

$$\text{of } \eta\text{: } \lambda,\ \mu,\ \nu,$$

$$\text{of } \zeta\text{: } \frac{1}{\sqrt{1 + p_1^2 + q_1^2}},\ \frac{p_1}{\sqrt{1 + p_1^2 + q_1^2}},\ \frac{q_1}{\sqrt{1 + p_1^2 + q_1^2}},$$

we note the relations

$$\begin{aligned} \alpha + p_1 \beta + q_1 \gamma &= 0, \\ \lambda + p_1 \mu + q_1 \nu &= 0, \\ \beta\nu - \gamma\mu &= \frac{1}{\sqrt{1 + p_1^2 + q_1^2}}. \end{aligned} \tag{12}$$

The coördinates u, v of b_1 in the plane π_2 are connected with the space coördinates δx_2, δy_2, δz_2 as follows:

$$\begin{aligned} u &= a\delta x_2 + b\delta y_2 + c\delta z_2 \\ v &= l\delta x_2 + m\delta y_2 + n\delta z_2. \end{aligned}$$

Hence by (10),

$$\begin{aligned} u = (a + p_2 b + q_2 c)\,\delta x_2 &+ [b\eta_1(x_2) + c\zeta_1(x_2)]\,\delta p_1 + [b\eta_2(x_2) + c\zeta_2(x_2)]\,\delta q_1 \\ v = (l + p_2 m + q_2 n)\,\delta x_2 &+ [m\eta_1(x_2) + n\zeta_1(x_2)]\,\delta p_1 \\ &+ [m\eta_2(x_2) + n\zeta_2(x_2)]\,\delta q_1; \end{aligned}$$

but by (11) the coefficients of δx_2 are zero, so that the equations connecting u, v with δp_1, δq_1 are

$$\begin{aligned} u &= [b\eta_1(x_2) + c\zeta_1(x_2)]\,\delta p_1 + [b\eta_2(x_2) + c\zeta_2(x_2)]\,\delta q_1 \\ v &= [m\eta_1(x_2) + n\zeta_1(x_2)]\,\delta p_1 + [m\eta_2(x_2) + n\zeta_2(x_2)]\,\delta q_1. \end{aligned} \tag{13}$$

For temporary expediency we call the coefficients in (13) A, B, C, D, writing these equations as

$$\begin{aligned} u &= A\delta p_1 + B\delta q_1 \\ v &= C\delta p_1 + D\delta q_1. \end{aligned} \tag{13'}$$

The next step is to pass from δp_1, δq_1 as coördinates for directions through a to ξ, η. ξ is the cosine of the angle between $1 : p_1 + \delta p_1 : q_1 + \delta q_1$ and α, β, γ, hence

$$\xi = \frac{\alpha + \beta(p_1 + \delta p_1) + \gamma(q_1 + \delta q_1)}{\sqrt{1 + p_1^2 + q_1^2}} = \frac{\beta\delta p_1 + \gamma\delta q_1}{\sqrt{1 + p_1^2 + q_1^2}},$$

on account of the first equation (12). In the same way,

$$\eta = \frac{\lambda + \mu(p_1 + \delta p_1) + \nu(q_1 + \delta q_1)}{\sqrt{1 + p_1^2 + q_1^2}} = \frac{\mu\delta p_1 + \nu\delta q_1}{\sqrt{1 + p_1^2 + q_1^2}},$$

by the second of the equations (12).

Solving for δp_1, δq_1, we have

$$\delta p_1 = (1 + p_1^2 + q_1^2)(\nu\xi - \gamma\eta),$$
$$\delta q_1 = (1 + p_1^2 + q_1^2)(-\mu\xi + \beta\eta),$$

wherein we have used the third equation (12).

Carrying these values for δp_1, δq_1 into (13′), there is obtained for the linear correspondence between ξ, η and u, v:

$$\begin{aligned} u &= (1 + p_1^2 + q_1^2)\{(\nu A - \mu B)\xi - (\gamma A - \beta B)\eta\}, \\ v &= (1 + p_1^2 + q_1^2)\{(\nu C - \mu D)\xi - (\gamma C - \beta D)\eta\}. \end{aligned} \tag{14}$$

We have said that $V(a, b)$ is the determinant of this correspondence. So

$$V(a, b) = (1 + p_1^2 + q_1^2)^2 \begin{vmatrix} \nu & \mu \\ \gamma & \beta \end{vmatrix} \cdot \begin{vmatrix} A & B \\ C & D \end{vmatrix}.$$

Introducing the expansions of A, B, C, D as in (13), we obtain

$$V(a, b) = (1 + p_1^2 + q_1^2)^2 \begin{vmatrix} \nu & \mu \\ \gamma & \beta \end{vmatrix} \cdot \begin{vmatrix} b & c \\ m & n \end{vmatrix} \cdot \begin{vmatrix} \eta_1(x_2) & \eta_2(x_2) \\ \zeta_1(x_2) & \zeta_2(x_2) \end{vmatrix},$$

and then, by reference to (11) and (12),

$$V(a, b) = \frac{(1 + p_1^2 + q_1^2)^{3/2}}{(1 + p_2^2 + q_2^2)^{1/2}} \begin{vmatrix} \eta_1(x_2) & \eta_2(x_2) \\ \zeta_1(x_2) & \zeta_2(x_2) \end{vmatrix}. \tag{15$_1$}$$

From (15$_1$) $V(b, a)$ is at once deducible by the systematic interchange of a and b:

$$V(b, a) = \frac{(1 + p_2^2 + q_2^2)^{3/2}}{(1 + p_1^2 + q_1^2)^{1/2}} \begin{vmatrix} \eta_3(x_1) & \eta_4(x_1) \\ \zeta_3(x_1) & \zeta_4(x_1) \end{vmatrix}. \tag{15$_2$}$$

13. **Expression for $W(a, b)$.** The preceding formulas show that the determination of $V(a, b)$ requires in general the solution of a system of two linear differential equations of the second order. But, as in the two-dimensional

theory, it appears that $W(a,b)$, on the contrary, can be expressed by a quadrature.

For, by division of (15_1) by (15_2),

$$W(a,b) = \frac{V(a,b)}{V(b,a)} = \frac{(1+p_1^2+q_1^2)^2}{(1+p_2^2+q_2^2)^2} \frac{\begin{vmatrix} \eta_1(x_2) & \eta_2(x_2) \\ \zeta_1(x_2) & \zeta_2(x_2) \end{vmatrix}}{\begin{vmatrix} \eta_3(x_1) & \eta_4(x_1) \\ \zeta_3(x_1) & \zeta_4(x_1) \end{vmatrix}};$$

and it has been shown at the end of § 11 that

$$\frac{\begin{vmatrix} \eta_1(x_2) & \eta_2(x_2) \\ \zeta_1(x_2) & \zeta_2(x_2) \end{vmatrix}}{\begin{vmatrix} \eta_3(x_1) & \eta_4(x_1) \\ \zeta_3(x_1) & \zeta_4(x_1) \end{vmatrix}} = e^{\int_{x_1}^{x_2}(F_{y'}+G_{z'})\,dx}.$$

Therefore

$$W(a,b) = \frac{(1+p_1^2+q_1^2)^2}{(1+p_2^2+q_2^2)^2} e^{\int_{x_1}^{x_2}(F_{y'}+G_{z'})\,dx}.$$

An equivalent form is:

$$W(a,b) = e^{\int_{x_1}^{x_2}\left(F_{y'}+G_{z'}-4\frac{y'F+zG'}{1+y'^2+z'^2}\right)dx}. \tag{16}$$

14. **The invariance of** $(\partial\gamma_1/\partial\theta_1)+(\partial\gamma_2/\partial\theta_2)$. It is desirable to obtain an expression of $W(a,b)$ in geometrically intrinsic terms. For this, we must find a quantity to play the rôle of the $\partial\gamma/\partial\theta$ of the two-dimensional theory. Such a quantity is furnished by the following considerations.

Given any family of ∞^4 curves in space,

$$y'' = F(x,y,z,y',z')$$
$$z'' = G(x,y,z,y',z'),$$

each point and direction (lineal element) define a curve. Let O, Ot be any point and direction of space, determining the curve C.

Construct a rectangular axis system Ot, Ou, Ov of which Ot is one of the axes. In this, it is to be emphasized, there is one degree of arbitrariness, for the axis system may be rotated freely about Ot.

The u and t axes define a pencil of directions, and accordingly a pencil of curves. These form a surface S_1 tangent to the plane ut. In the same way, the v axis defines with the t axis a pencil of curves, which form a surface S_2 tangent to the plane vt.

The surfaces S_1 and S_2 intersect in the curve C. Introducing here the idea of geodesic curvature, we direct attention to the fact that the geodesic curvature of a curve upon a surface is relative to both surface and curve. Let the geodesic curvature at O of C be γ_1 upon S_1, and γ_2 upon S_2.

Regard S_1. It is covered with a pencil of curves issuing from O. Let $\partial\gamma_1/\partial\theta_1$ denote the rate at which the geodesic curvature changes in this pencil as we pass from C to the infinitesimally adjacent curves. And let $\partial\gamma_2/\partial\theta_2$ denote the corresponding quantity for the surface S_2.

Then we state the

THEOREM. *The sum* $(\partial\gamma_1/\partial\theta_1) + (\partial\gamma_2/\partial\theta_2)$ *is independent of the one degree of freedom involved in the choice of the trirectangular system* t, u, v.

To prove this, suppose the curve family referred to t, u, v as x, y, z axes; then, taking advantage of the fact that geodesic curvature is equal to tangential curvature, we have

$$\frac{\partial\gamma_1}{\partial\theta_1} = F_{y'}, \qquad \frac{\partial\gamma_2}{\partial\theta_2} = G_{z'}.$$

If the t, u, v system is rotated about t through an angle φ, we find that, relative to the new trirectangular system,

$$\frac{\partial\gamma_1}{\partial\theta_1} = \cos^2\varphi F_{y'} + \sin\varphi\cos\varphi(F_{z'} + G_{y'}) + \sin^2\phi G_{z'},$$

$$\frac{\partial\gamma_2}{\partial\theta_2} = \sin^2\varphi F_{y'} - \sin\varphi\cos\varphi(F_{z'} + G_{y'}) + \cos^2\varphi G_{z'}.$$

Adding, the angle φ disappears:

$$\frac{\partial\gamma_1}{\partial\theta_1} + \frac{\partial\gamma_2}{\partial\theta_2} = F_{y'} + G_{z'},$$

whence the invariantive property of $(\partial\gamma_1/\partial\theta_1) + (\partial\gamma_2/\partial\theta_2)$ as stated.

With this result established, the formula (16) can be given the form:

$$W(a, b) = \frac{V(a, b)}{V(b, a)} = e^{\int_a^b \left(\frac{\partial\gamma_1}{\partial\theta_1} + \frac{\partial\gamma_2}{\partial\theta_2}\right) ds}. \tag{17}$$

15. **The case of symmetric** $V(a, b)$. The families of ∞^4 curves in space for which $V(a, b)$ is symmetric in its two arguments are found immediately from considering the formulas (16), (17).

THEOREM. *The curve families for which*

$$V(a, b) \equiv V(b, a)$$

are those for which

$$\frac{\partial\gamma_1}{\partial\theta_1} + \frac{\partial\gamma_2}{\partial\theta_2} \equiv 0.*$$

* A more graphical form of this condition is as follows: We can construct an indicatrix to show the variation of curvature; namely, O, Ot being any point and direction, by laying off on every ray Ou perpendicular to Ot a length proportional to $(\partial\gamma/\partial\theta)^{-1/2}$ relative to the pencil defined by Ou, Ot. The indicatrix is in every case a conic with O as center. When $V(a, b)$ is symmetric every indicatrix is an equilateral hyperbola, and conversely.

How is the property $V(a,b) \equiv V(b,a)$ to be recognized in a given family of ∞^4 curves from the analytic form of the differential equations? According to (16) the necessary and sufficient condition for the property in question is

$$F_{y'} + G_{z'} - 4\,\frac{y'F + z'G}{1 + y'^2 + z'^2} = 0.$$

This equation is transformable into

$$\frac{\partial}{\partial y'}\left[\frac{F}{(1+y'^2+z'^2)^2}\right] + \frac{\partial}{\partial z'}\left[\frac{G}{(1+y'^2+z'^2)^2}\right] = 0.$$

Hence the result:

The families of ∞^4 curves that have the property $V(a,b) \equiv V(b,a)$ are characterized by differential equations of the form

$$y'' = (1 + y'^2 + z'^2)^2\,\Omega_1,$$
$$z'' = (1 + y'^2 + z'^2)^2\,\Omega_2,$$

where Ω_1, Ω_2 are any two functions of x, y, z, y', z' that obey the relation

$$\frac{\partial \Omega_1}{\partial y'} + \frac{\partial \Omega_2}{\partial z'} = 0. \tag{18}$$

The general solution of (18) is

$$\Omega_1 = \frac{\partial}{\partial z'}\phi(x, y, z, y', z'),$$
$$\Omega_2 = -\frac{\partial}{\partial y'}\phi(x, y, z, y', z'),$$

where ϕ is any function of its five arguments. The type of curve system here under consideration depends therefore on one arbitrary function of five arguments, whereas the general system of ∞^4 curves in space depends on two such functions.

16. **Straubel's theorem; its converse.** Straubel's theorem for three-dimensional space results from applying the formula (16) for $W(a,b)$ to the case of a natural family of curves. Such a family, consisting of the paths of light in an isotropic optical medium, is determined as the system of extremals of $\int \nu(x,y,z)\,ds$, ν being the index of refraction,—or by the equivalent differential equations

$$y'' = (L_y - y'L_x)(1 + y'^2 + z'^2),$$
$$z'' = (L_z - z'L_x)(1 + y'^2 + z'^2), \tag{19}$$

where $L = \log \nu$.*

* Cf. E. Kasner, loc. cit.

Applying (16) to the equations (19), we find

$$\frac{V(a,b)}{V(b,a)} = \frac{\nu^2(a)}{\nu^2(b)}. \tag{20}$$

Consider the converse question. In connection with what systems of ∞^4 curves can a function of position ν be defined so that the relation (20) shall subsist? By use of (16), it turns out that this is possible whenever the differential equations are of the form

$$\begin{aligned} y'' &= (L_y - y' L_x)(1 + y'^2 + z'^2) + (1 + y'^2 + z'^2)^2 \Omega_1, \\ z'' &= (L_z - z' L_x)(1 + y'^2 + z'^2) + (1 + y'^2 + z'^2)^2 \Omega_2, \end{aligned} \tag{21}$$

where Ω_1, Ω_2 are any two functions of x, y, z, y', z' subject to the condition

$$\frac{\partial \Omega_1}{\partial y'} + \frac{\partial \Omega_2}{\partial z'} = 0.$$

The Straubel property is therefore not characteristic of natural families.

17. **Flat (Euclidean) n-dimensional space.** The preceding theorems admit of easy generalization to a flat n-space. Using as notation for the coördinates $x, y_1, y_2, \cdots, y_{n-1}$, a system of $n-1$ differential equations of the second order,

$$y_i'' = F_i(x, y_j; y_j') \qquad (i, j = 1, 2, \cdots, n-1) \tag{22}$$

will define a system of ∞^{2n-2} curves. Such a system will have the property $V(a,b) \equiv V(b,a)$ when the differential equations are of the form

$$y_i'' = (1 + y_1'^2 + \cdots + y_{n-1}'^2)^{(n+1)/2} \Omega_i \quad (i = 1, 2, \cdots, n-1), \tag{23}$$

where the Ω's are any functions of the x, y_j, y_j' that obey the relation

$$\frac{\partial \Omega_1}{\partial y_1'} + \frac{\partial \Omega_2}{\partial y_2'} + \cdots + \frac{\partial \Omega_{n-1}}{\partial y_{n-1}'} = 0. \tag{24}$$

The Straubel property, which for n-space is

$$\frac{V(a,b)}{V(b,a)} = \frac{\nu^{n-1}(a)}{\nu^{n-1}(b)},$$

is found to be characteristic of the families defined by differential equations of the form:

$$\begin{aligned} y_i'' = {} & (L_{y_i} - y_i' L_x)(1 + y_1'^2 + \cdots + y_{n-1}'^2) \\ & + (1 + y_1'^2 + \cdots + y_{n-1}'^2)^{(n+1)/2} \Omega_i \\ & (i = 1, 2, \cdots, n-1), \end{aligned} \tag{25}$$

where the Ω's are subject to the condition (24).

We note that the general solution of (24) is obtained by taking any $(n-2)$ functions

$$\phi_1, \phi_2, \cdots, \phi_{n-2}$$

of the arguments x, y_j, y_j' and setting the Ω's equal to the jacobians:*

$$\Omega_1 = \frac{\partial(\phi_1, \phi_2, \cdots, \phi_{n-2})}{\partial(y_2', y_3', \cdots, y_{n-1}')}, \qquad \Omega_2 = -\frac{\partial(\phi_1, \phi_2, \cdots, \phi_{n-2})}{\partial(y_1', y_3', \cdots, y_{n-1}')}, \qquad \text{etc.}$$

The families with symmetric $V(a, b)$ depend therefore on one less arbitrary function of the $2n-1$ arguments x, y_j, y_j' than the general family of ∞^{2n-2} curves.

III. Theory for a general (curved, non-euclidean) variety of n dimensions

18. **The invariance of $\Sigma(\partial\gamma_i/\partial\theta_i)$. Formula for $W(a, b)$.** We extend our developments, finally, to a general variety V_n, one in which the squared element of length is defined by the general quadratic form,

$$ds^2 = \sum a_{ik}\, dx_i\, dx_k.$$

The first step is to generalize the theorem of part II concerning the invariance of $(\partial\gamma_1/\partial\theta_1) + (\partial\gamma_2/\partial\theta_2)$. We are considering a system of ∞^{2n-2} curves in V_n, one for each point and direction. Let the point O and direction Ot define the curve C. Then let a system of n rectangular directions be constructed of which Ot is one: $Ot, Ot_1, \cdots, Ot_{n-1}$. Each Ot_i determines with Ot a pencil of directions, therefore a pencil of curves, which form a two-spread $V_2^{(i)}$. There arise in this way $n-1$ V_2's, all intersecting in the curve C. On each $V_2^{(i)}$, C has at O a definite geodesic curvature γ_i, which changes at a definite rate $\partial\gamma_i/\partial\theta_i$ as we pass from C to the infinitesimally adjacent curves upon $V_2^{(i)}$.

Now, in the construction of the rectangular system Ot_i it is seen that there exist $\frac{1}{2}(n-1)(n-2)$ degrees of freedom. Hence the significance of the

Theorem. *The sum*

$$\sum_{i=1}^{i=n-1} \frac{\partial\gamma_i}{\partial\theta_i}$$

is independent of the $\frac{1}{2}(n-1)(n-2)$ degrees of freedom involved in the construction of the rectangular system $Ot, Ot_1, \cdots, Ot_{n-1}$.

Upon this result we can then establish the theorem:

$$W(a, b) = e^{\int_a^b \sum_{i=1}^{n-1} \frac{\partial\gamma_i}{\partial\theta_i} ds}. \tag{1}$$

From the form of the last equation there follow for a general space the same

* See De La Vallée Poussin, *Cours d'Analyse*, vol. 2, p. 302.

corollaries as in §§ 4, 5 of the theory for the plane. It follows also that the necessary and sufficient condition for

$$V(a, b) \equiv V(b, a)$$

is

$$\sum_{i=1}^{i=n-1} \frac{\partial \gamma_i}{\partial \theta_i} \equiv 0. \tag{2}$$

19. **Geodesics. Levi-Civita's theorem.** Consider the most important example of ∞^{2n-2} curves in V_n—the geodesics. A geodesic in V_n is a fortiori a geodesic upon any sub-variety V_m upon which it may lie. Recalling the meaning of γ_i as defined in the preceding section, we see that for the geodesics we have, separately and identically,

$$\gamma_1 = 0, \qquad \gamma_2 = 0, \qquad \cdots, \qquad \gamma_{n-1} = 0,$$

and hence, separately and identically,

$$\frac{\partial \gamma_1}{\partial \theta_1} = 0, \qquad \frac{\partial \gamma_2}{\partial \theta_2} = 0, \qquad \cdots, \qquad \frac{\partial \gamma_{n-1}}{\partial \theta_{n-1}} = 0.$$

From these equations there follows, according to (2),

Levi-Civita's Theorem.* *The geodesics of any n-dimensional variety have the property* $V(a, b) \equiv V(b, a)$.

Levi-Civita's result thus falls as a special case under the theorem stated above in connection with the equation (2).

20. **Conformal representation. Straubel's theorem and its generalization.** In conclusion, we consider Straubel's theorem for a general variety V_n. Taking the Straubel relation

$$\frac{V(a, b)}{V(b, a)} = \frac{\nu^{n-1}(a)}{\nu^{n-1}(b)}, \tag{3}$$

we inquire as to the most general family of ∞^{2n-2} curves in V_n in connection with which a point-function ν can be defined so that the stated relation shall hold.

To this end, conformal representation furnishes the easiest method. Let the manifold V_n, of which the fundamental form is

$$ds^2 = \sum a_{ik}\, dx_i\, dx_k,$$

be represented upon a second manifold V_n' of which the fundamental form is

$$ds_1^2 = \nu^2 \sum a_{ik}\, dx_i\, dx_k$$

so that points with the same coördinates correspond. Since $ds_1 = \nu ds$, the mapping so defined is conformal with modulus of conformality ν.

* See the introduction.

The behavior of $V(a, b)$ under the conformal transformation is seen to be as follows:

$$V(a_1, b_1) = \nu^{n-1}(b)\, V(a, b), \tag{4}$$

$$V(b_1, a_1) = \nu^{n-1}(a)\, V(b, a). \tag{5}$$

By division,

$$\frac{V(a_1, b_1)}{V(b_1, a_1)} = \frac{\nu^{n-1}(b)}{\nu^{n-1}(a)} \frac{V(a, b)}{V(b, a)}. \tag{6}$$

Hence if in V_n we have the condition (3), then in V_n' we shall have

$$V(a_1, b_1) = V(b_1, a_1), \tag{7}$$

and conversely.

The relation (7) holds in particular for the geodesics of V_n' (Levi-Civita's theorem). These are the extremals of

$$\int ds_1 = \text{min.};$$

the image curves in V_n are therefore the extremals of

$$\int \nu ds = \text{min.};$$

they are, in other words, a natural family. Thus all natural families have the Straubel property.

But the property (7) belongs not only to the geodesics of V_n',—it holds for every system of ∞^{2n-2} curves that satisfy the condition $\Sigma(\partial\gamma_i/\partial\theta_i) \equiv 0$. Hence the Straubel property is not restricted to natural families, that is to the conformal images of geodesics, but is true of the more inclusive type that results by conformal mapping from any family with the symmetric property $V(a, b) \equiv V(b, a)$, or its equivalent $\Sigma(\partial\gamma_i/\partial\theta_i) \equiv 0$.

COLUMBIA UNIVERSITY

PROPERTIES OF THE SOLUTIONS OF CERTAIN FUNCTIONAL DIFFERENTIAL EQUATIONS*

BY

WILLIAM BENJAMIN FITE

INTRODUCTION

The functional differential equations here under discussion have already been considered in a general way by Fr. Polussuchin who in her dissertation† reduced the solution of a more comprehensive class of equations to the solution of integral equations of the second kind. In the more detailed treatment of the present paper the existence of solutions of certain equations is established in the first part by the method of successive approximations. Some of the properties of the solutions whose existence is thus established are discussed in the second part.

I. AN EXISTENCE THEOREM

Consider the equation

$$(1) \qquad y^{(n)}(x) + \sum_{i=1}^{n} p_i(x) y^{(n-i)}(x) + r(x) y[\phi(x)] = 0,$$

where, within the closed interval (a, b) containing the point $x = c$, the functions $p_i(x)$ and $r(x)$ are continuous and $\phi(x)$ satisfies the conditions:

(1) $\phi(x)$ is continuous and within (a, b),

(2) $|\phi(x) - c| \leqq |x - c|$.

We proceed to establish the existence of solutions of (1) by the familiar method of successive approximations. We shall sketch the details for the case $n = 3$.

$$(2) \quad y'''(x) + p_1(x) y''(x) + p_2(x) y'(x) + p_3(x) y(x) + r(x) y[\phi(x)] = 0.$$

We wish to establish the existence of a solution y of (2) such that $y(c) = u_0$, $y'(c) = v_0$, and $y''(c) = w_0$, where u_0, v_0, and w_0 are arbitrarily assigned numbers.

* Presented to the Society April 26 and December 31, 1919.

† *Über eine besondere Klasse von differentialen Funktionalgleichungen.* Inaugural-dissertation, Zürich, 1910.

Let $P_i (i = 1, 2, 3)$ and R be four numbers such that within (a, b)

$$|p_i(x)| \leqq P_i \qquad \text{and} \qquad |r(x)| \leqq R.$$

Put $u = y$, $v = y'$, and $w = y''$. Then (2) becomes

$$u'(x) = v(x); \qquad v'(x) = w(x);$$

$$w'(x) = -p_1(x)w(x) - p_2(x)v(x) - p_3(x)u(x) - r(x)u[\phi(x)].$$

We define the three series of functions $u_j(x)$, $v_j(x)$, and $w_j(x)$ $(j = 1, 2, \cdots)$ in the following way:

$$u_1'(x) = v_0; \qquad v_1'(x) = w_0;$$
$$w_1'(x) = -p_1(x)w_0 - p_2(x)v_0 - p_3(x)u_0 - r(x)u_0;$$

and, in general,

$$u_j'(x) = v_{j-1}(x); \qquad v_j'(x) = w_{j-1}(x);$$

$$w_j'(x) = -p_1(x)w_{j-1}(x) - p_2(x)v_{j-1}(x) - p_3(x)u_{j-1}(x) - r(x)u_{j-1}'[\phi(x)];$$

$$u_j(c) = u_0, \qquad v_j(c) = v_0, \qquad w_j(c) = w_0.$$

If we choose a number A such that $|u_0|$, $|v_0|$, and $|w_0|$ do not exceed A, then $|u_1(x) - u_0| \leqq A|x - c|$, and, in general,

$$|u_j(x) - u_{j-1}(x)| \leqq M^{j-2} A \frac{|x-c|^j}{j!} \qquad (j > 1),$$

$$|v_j(x) - v_{j-1}(x)| \leqq M^{j-1} A \frac{|x-c|^j}{j!} \qquad (j \geqq 1),$$

$$|w_j(x) - w_{j-1}(x)| < M^j A \frac{|x-c|^j}{j!} \qquad (j \geqq 1),$$

where

$$\sum_{i=1}^{3} P_i + R < M, \qquad M \geqq 1,$$

and therefore

$$P_1 M + P_2 + P_3 + R < M^2$$

and

$$P_1 M^2 + P_2 M + P_3 + R < M^3.$$

It should be borne in mind that

$$|u_j[\phi(x)] - u_{j-1}[\phi(x)]| \leqq M^{j-2} A \frac{|\phi(x) - c|^j}{j!} \leqq M^{j-2} A \frac{|x-c|^j}{j!},$$

when $j > 1$ and that a similar inequality holds when $j = 1$.

The conclusion as to the existence and uniqueness of a solution satisfying the given initial conditions at the point $x = c$ follows as in the case of differential equations.* This conclusion can obviously be extended to the equation (1) of order n. The conclusion still holds if we remove from the function $\phi(x)$ the restriction (2) and assume instead either that

$$M(b-a) < 1,\ M \geqq 1,\ \text{or}\ b-a < 1,\ M < 1.$$

If y and z are two solutions of (1) such that each of the differences $y^{(i)} - z^{(i)}$ $(i = 0, 1, \cdots, n-1)$ vanishes somewhere within an interval containing the point $x = c$, it can be shown as in the analogous case for differential equations† that there is a minimum possible length for this interval. The equation

$$y''(x) + \frac{5}{2}y(x) + \frac{3}{2}y(\pi - x) = 0$$

has the solutions $y = \cos x$ and $y = \cos 2x$, and these functions, as well as their first derivatives, are equal for $x = 0$. This shows the importance of the restriction that the interval we are considering shall contain the point $x = c$, which must here be the point $x = \pi/2$.

Moreover no non-identically vanishing solution of (1) and its first $n-1$ derivatives can vanish within a sufficiently small interval containing the point $x = c$. Hence if a solution vanishes n times within this interval, it vanishes identically here.

The following theorem is a direct consequence of the preceding discussion:

THEOREM I: *Within a properly restricted interval containing the point $x = c$ equation* (1) *has exactly n linearly independent solutions.*

The same method can of course also be used to establish the existence of solutions of non-homogeneous equations of the form

$$y^{(n)}(x) + \sum_{i=1}^{n} p_i(x)\, y^{(n-i)}(x) + r(x)\, y[\phi(x)] = g(x).$$

II. PROPERTIES OF THE SOLUTIONS

Consider first the equation

$$y^{(n)}(x) + p(x)\, y^{(n-1)}(x) + r(x)\, y(k-x) = 0, \tag{3}$$

where n is even and $r(x) > 0$ for the values of x under consideration. Here the c of the preceding discussion is $k/2$. It follows from Theorem I that within a properly chosen interval (a, b) with $k/2$ as center equation (3) has n linearly independent solutions. If we select $n-1$ arbitrary, distinct points

* See, for example, Goursat, *Cours d'analyse, 3d ed.*, vol. 2, p. 377.

† Fite, these Transactions, vol. 19 (1918), p. 351.

within such an interval, there is therefore a solution y that vanishes at these points.

Now y must change sign at each of these points, since otherwise y' would vanish at least $n-1$ times in (a, b), and the first $n-1$ derivatives of y, as well as y itself, would vanish in this interval. But it has been shown that this can happen only in case y vanishes identically. Moreover y will not vanish at any other point of the interval.

We proceed to show that y will not vanish at any point outside of (a, b). Let x_1 be the extreme left hand point in (a, b) at which y changes sign. If y vanished at any point to the left of a, let x_0 be the nearest such point to a, and suppose that y is negative between x_0 and x_1. Then as x increases from values a little greater than x_0 to b, y', beginning with a negative value, would change sign $n-1$ times; and $y^{(n-2)}$ would change from positive to negative and back to positive. Moreover the change from positive to negative would take place to the left of a, since otherwise $y^{(n-2)}$ would change sign twice within (a, b) and therefore $y^{(n-1)}$ would vanish in this interval together with y and its first $n-2$ derivatives. Then $y^{(n-1)}$ must be positive in (a, b), and negative a little to the left of a. It would therefore vanish at some point c in (x_0, a), while $y^{(n)}(c)$ would be positive and $y(k-c)$ would be negative. Hence y would change sign for some value of x greater than b. But for values of x a little less than b, y and its first $n-1$ derivatives would all be positive. Hence as x increases from b, $y^{(n-1)}$ would vanish before y does. But for the value of x at which this happens, $y(k-x)<0$. Hence $y^{(n)}(x)>0$. But $y^{(n-1)}(x)$ cannot pass from a positive value to zero when $y^{(n)}(x)>0$. Hence y does not vanish to the left of a. If it vanished to the right of b, a similar argument shows that it would also vanish to the left of a. Hence

THEOREM II: *If equation* (3) *is of even order, no solution that vanishes at* $n-1$ *distinct points within a sufficiently small interval with* $x=k/2$ *as center can vanish at any other point of the interval within which the existence of solutions was established in Part I.*

In case $p(x)$ and $r(x)$ are continuous, and $r(x)>0$, for all finite values of x, the argument shows furthermore that y increases without limit as x increases from b. As an example we cite the equation $y''(x)+y(-x)=0$, which has the solution $y=e^x-e^{-x}$.

Suppose now that y_1 and y_2 are linearly independent solutions of (3) when $n=2$. We can assume that $y_1(k/2)=y_2(k/2)$. Then the solution $y=y_1-y_2$ changes sign at $k/2$, but at no other point within the interval of existence of the solutions. That is, two independent solutions that are equal for $x=k/2$ are not equal for any other value of x within this interval. It follows from this that if three consecutive changes of sign of y_1 on the same side of $k/2$ are at $x_1, x_2, x_3 (x_1<x_2<x_3)$, then y_2 does not change sign in

both of the intervals (x_1, x_2) and (x_2, x_3). Since the points at which a solution changes sign are not affected by multiplying the solution by a constant, the statement just made concerning the changes of sign of y_1 and y_2 applies to any two independent solutions. Moreover—and this result is analogous to Sturm's theorem of separation for the roots of solutions of linear homogeneous differential equations of order 2,—if x_1 and x_2 are two consecutive zeros of y_1 on opposite sides of $k/2$, every independent solution, as y_2, changes sign in (x_1, x_2). If it changes sign more than once in this interval, the points at which these changes occur are on the same side of $k/2$, since otherwise y_1 would change sign between the two of these points that are adjacent to $k/2$. If it changes sign once within the interval between any two consecutive changes of sign of y_1, it changes sign an even number of times in this interval, except when $k/2$ is in the interval, and then the number of changes of sign is odd.

We shall now consider the equation

$$y^{(n)}(x) + r(x)y(k - x) = 0, \tag{4}$$

where $r(x)$ is continuous for all finite values of x and greater than the positive number h for all sufficiently large positive and negative values of x. We shall find certain points of similarity with the corresponding type of differential equations and certain striking points of difference. It is necessary in the argument to distinguish between odd and even values of n.

(*a*) *n odd:* Suppose that a solution y does not change sign an unlimited number of times. We can then choose a value $x_1 (> k)$ such that y is positive or zero for all values of x greater than x_1,* and does not change sign for values of x less than $k - x_1$. If $y \geqq 0$ for these latter values of x, then $y^{(n)} \leqq 0$ for $x > x_1$, and $y^{(n-1)}$ would not increase as x increases from x_1. If it were negative for any such value of x, it would be negative for all greater values, and y would ultimately change sign. But this is contrary to our supposition. Hence $y^{(n-1)}$ would approach a limit which is equal to, or greater than, zero; and therefore $y^{(n)}$ would come indefinitely near to zero. This in turn would require that y should come indefinitely near to zero as x decreases from $k - x_1$. But as x decreases in this way none of the first $n - 1$ derivatives of y can change sign more than a limited number of times, since otherwise $y^{(n)}$ would change sign for a value of x less than $k - x_1$, and y would change sign for a value of x greater than x_1. Hence for a properly chosen x_2 each of the first n derivatives of y would have a fixed sign for all values of $x < x_2$. For these values of x, y' would be positive and would approach zero as x approaches $-\infty$. Hence y'' would also be positive, as would also all the derivatives up to, and including, $y^{(n)}$. But this is contrary to the supposition that $y \geqq 0$ for $x > x_1$.

* The argument here and farther on assumes that y is not identically zero for large values of x. It is not difficult to justify this assumption.

If, on the other hand, $y \leqq 0$ for $x < k - x_1$, we should have $y^{(n)} \geqq 0$ for $x > x_1$. If $y^{(n-1)}$ became positive for any of these latter values of x, it would remain positive for all greater values and y would increase indefinitely. Then $y^{(n)}$ would approach $-\infty$ as x decreases indefinitely, and y would therefore, under the same circumstances, become positive, since n is odd. But this is contrary to our supposition. If $y^{(n-1)}$ did not become positive, it would approach a limit and $y^{(n)}$ would come indefinitely near to zero as x approaches $+\infty$. This would require that y come indefinitely near to zero as x approaches $-\infty$, and, as before, for values of x less than an assignable x_2, each of the first n derivatives of y would approach zero as x approaches $-\infty$. This would require y to approach zero as x approaches $+\infty$. Now, by supposition, $y^{(n)}$ is positive or zero and $y^{(n-1)}$ is negative for sufficiently large positive values of x, and the successive derivatives from $y^{(n)}$ down to y' inclusive are of alternate signs, since otherwise y would either increase without limit, or change sign, as x increases. This would require y' to be positive—a result which is inconsistent with the assumption that y be positive and approach zero as x approaches $+\infty$. In this argument we have assumed $n > 1$. But it is obvious that the same conclusion holds for $n = 1$. Hence *y changes sign an unlimited number of times in case n is odd.*

(*b*) *n even:* The situation is essentially different when n is even, for we have seen that there are solutions which change sign exactly $n - 1$ times.

Suppose now that a solution y changed sign just an even number of times. We could assume that $y \geqq 0$ for $x > x_1$ and $x < k - x_1$, provided that x_1 is a properly chosen positive number. For $x > x_1$ the derivatives $y^{(n)}, y^{(n-1)}, \cdots, y'$ would be alternately negative and positive, since if two consecutive ones were negative, y would ultimately change sign, and if two consecutive ones were positive, y would increase without limit, and hence, for sufficiently large negative values of x, $y^{(n)}$ would be less than an assignable negative quantity and y would change sign contrary to our supposition. But if these derivatives were alternately negative and positive, y' would be positive, and we would have the same contradiction as before. This completes the proof of

THEOREM III: *If $r(x)$ is continuous for all finite values of x and greater than the positive number h for all sufficiently large positive and negative values of x, every solution of the equation*

$$y^{(n)}(x) + r(x)\,y(k - x) = 0$$

*changes sign an infinite number of times in case n is odd; if n is even every solution changes sign either an odd number of times, or an infinite number of times.**

* In order to compare these results with the results for differential equations of corresponding form, see Kneser, Mathematische Annalen, vol. 42 (1893), pp. 434–5, and Fite, loc. cit., p. 349.

For example, the equation

$$y''(x) + y(\pi - x) = 0$$

has the solutions $y = \sin x$ and $y = e^x - e^{\pi - x}$. No solution except the former changes sign an infinite number of times.

We now remove the restriction that r be greater than h and require merely that it be positive and continuous for the values of x under consideration. For any solution y of (4) we have

$$(5)\quad y(x) = y\left(\frac{k}{2}\right) + y'\left(\frac{k}{2}\right)\left(x - \frac{k}{2}\right) + \cdots + y^{(n-1)}\left(\frac{k}{2}\right)\frac{\left(x - \frac{k}{2}\right)^{n-1}}{(n-1)!} - r(x_0)\,y(k - x_0)\frac{\left(x - \frac{k}{2}\right)^{n}}{n!},$$

where x_0 is between x and $k/2$. If c is the first root of the equation

$$(6)\quad y\left(\frac{k}{2}\right) + y'\left(\frac{k}{2}\right)\left(x - \frac{k}{2}\right) + \cdots + y^{(n-1)}\left(\frac{k}{2}\right)\frac{\left(x - \frac{k}{2}\right)^{n-1}}{(n-1)!} = 0$$

that is greater than $k/2$ and y has no root for $k/2 < x < c$, then $y(k - c_0) \leqq 0$, where $k/2 < c_0 < c$, if we assume that either $y(k/2) > 0$ or $y(k/2) = 0$ and that the first derivative of y that does not vanish for $k/2$ is positive here. If d is the first root of (6) less than $k/2$, and y has no root for $d < x < k/2$, then $y(k - d_0) \leqq 0$, where $d < d_0 < k/2$, in case n is even. If (6) has no real root, and n is odd, the first root of y greater than $k/2$ is nearer to $k/2$ than the first root less than $k/2$.

THEOREM IV: *If equation* (6) *has a real root distinct from* $k/2$ *when* n *is even,* y *changes sign at a point nearer to* $k/2$ *than any such root of* (6). *When* n *is odd and* (6) *has a root greater than* $k/2$, y *changes sign at a point nearer to* $k/2$ *than any such root of* (6). *If this equation has no real root, and* n *is odd, the first root of* y *greater than* $k/2$ *is nearer to* $k/2$ *than the first root less than* $k/2$.

We have now to consider the solutions of (4) under the conditions that $r(x)$ is continuous for all finite values of x and less than the negative number $-h$ for all sufficiently large positive and negative values of x. As before, it is necessary to distinguish between odd and even values of n.

(*a*) n *odd:* Suppose that for $n > 1$ we have a solution y that changes sign just an even number of times, or not at all; that is, that $y \geqq 0$ for $x > x_1$ and $x < k - x_1$. For $x > x_1$, $y^{(n)} \geqq 0$, and if $y^{(n-1)}$ were positive or zero for any such value of x, y would ultimately increase without limit as x approaches $+\infty$. Then as x approaches $-\infty$, $y^{(n)}$ would increase without limit and $y^{(n-1)}$ would decrease without limit. Tracing the effect of this on the pre-

ceding derivatives down to the first one and to y, we see that the latter would ultimately change sign as x decreases from $k - x_1$. But this is contrary to our assumption. We assume then that $y^{(n-1)}$ is negative for $x > x_1$. As x increases, it would therefore approach a limit and $y^{(n)}$ would come indefinitely near to zero. This would require that y come indefinitely near to zero as x decreases from $k - x_1$. Moreover for all sufficiently large negative values of x each of the first n derivatives of y would have a fixed sign, and $y^{(n)}$ would come indefinitely near to zero as x decreases from $k - x_1$. Hence y would come indefinitely near to zero as x increases from x_1. Now we have seen that $y^{(n-1)} < 0$ when $x > x_1$. If then $y^{(n-2)}$ were zero or negative for such a value of x, it would be negative for all greater values of x, and y would change sign for a value of $x > x_1$. We must assume then that $y^{(n-2)} > 0$ for $x > x_1$. A continuation of this argument shows that under the given conditions y' would be positive for these values of x. But this is inconsistent with the conclusion just reached that y must come indefinitely near to zero as x increases from x_1. If $n = 1$ it would be impossible for y to change sign just an even number of times. We conclude therefore that y cannot change sign just an even number of times when n is odd.

Suppose now that y changed sign just an odd number of times—that is, that $y \geqq 0$ for $x > x_1$ and $y \leqq 0$ for $x < k - x_1$. Then $y^{(n)} \leqq 0$ and $y^{(n-1)} > 0$ for $x > x_1$. If $n > 1$ and $y^{(n-2)}$ were positive or zero for some such value of x, y would increase without limit as x approaches $+\infty$, and $y^{(n)}$ would increase without limit as x approaches $-\infty$. This would require that y decrease without limit under the same circumstances. Then $y^{(n)}$ would decrease without limit as x approaches $+\infty$. But this is inconsistent with the fact that $y^{(n-1)}$ remains positive under the same circumstances. We must assume then that $y^{(n-2)} < 0$ for $x > x_1$. This would require that $y^{(n-1)}$ approach zero and that $y^{(n)}$ come indefinitely near to zero as x approaches $+\infty$. Then y would come indefinitely near to zero as x approaches $-\infty$, and y' and $y^{(n)}$ would be negative for all sufficiently large negative values of x. But this is inconsistent with the fact that y is positive for $x > x_1$. If $n = 1$, y' would come indefinitely near to zero as x increases from x_1, and therefore y would come indefinitely near to zero as x decreases from $k - x_1$. But this is inconsistent with the fact that, for $x < k - x_1$, y is negative or zero and y' is positive or zero. Hence *when n is odd y' changes sign an infinite number of times.*

(*b*) *n even:* Suppose first that $y \geqq 0$ for $x > x_1$ and $y \leqq 0$ for $x < k - x_1$. Then, for $x > x_1$, $y^{(n)} \leqq 0$ and $y^{(n-1)} > 0$. If $n > 2$ and $y^{(n-2)}$ were positive or zero for such a value of x, y would increase without limit as x approaches $+\infty$ and $y^{(n)}$ would increase without limit as x approaches $-\infty$. This would require that y be positive for sufficiently large negative values of x,

contrary to our supposition. If $y^{(n-2)}$ were negative for $x > x_1$, $y^{(n-1)}$ would approach zero, and $y^{(n)}$ would come indefinitely near to zero, as x approaches $+\infty$. Then y would approach zero as x approaches $-\infty$. But this is impossible, since, for $x < k - x_1$, $y^{(n)} \geqq 0$. The argument is substantially the same when $n = 2$, since we could assume $y' > 0$ for $x > x_1$, and y greater than an assignable positive number for these values of x.

There are equations that have solutions, y, such that $y \geqq 0$ for $x > x_1$ and $x < k - x_1$. For example, the equation $y''(x) - y(-x) = 0$ has the solutions $y = e^x + e^{-x}$, which does not vanish at all, $y = \sin x$, which changes sign an infinite number of times, and $y = e^x + e^{-x} - a \sin x$, which changes sign a given even number of times for a properly chosen value of a.

THEOREM V: *Every solution of equation* (4) *when* $r(x)$ *is continuous for all finite values of* x *and less than the negative number* $-h$ *for all sufficiently large positive and negative values of* x *changes sign an infinite number of times in case* n *is odd; in case* n *is even every solution changes sign an infinite number of times or an even number.**

COLUMBIA UNIVERSITY

* In contrast with this result, compare Kneser, loc. cit., p. 413, and Bôcher, these Transactions, vol. 3 (1902), p. 199, theorem IV, for the properties of differential equations of corresponding form.

NOTE ON A CLASS OF POLYNOMIALS OF APPROXIMATION*

BY

DUNHAM JACKSON

1. **Introduction.** In a recent paper† it was shown that if $f(x)$ is a given continuous function in the interval $a \leqq x \leqq b$, n a given positive integer, and m a given real number greater than 1, there exists one and just one polynomial $\phi(x)$, of degree n or lower, which reduces to a minimum the value of the integral

$$\int_a^b |f(x) - \phi(x)|^m \, dx.$$

The purpose of this note is to establish the truth of the same proposition in the case that $m = 1$, for which the proof is considerably less simple.

The function $\phi(x)$ in the earlier paper was, more generally, a linear combination, with constant coefficients, of an arbitrarily given set of linearly independent continuous functions. The existence of at least one minimizing function is proved with the same degree of generality here. The argument involves no new difficulty, and in fact is slightly simpler than for $m > 1$. For the proof of uniqueness, however, $\phi(x)$ is essentially a polynomial as indicated,‡ though a corresponding treatment could be given for other approximating functions, such as finite trigonometric sums, which are similarly determined by their roots.

2. **Existence of an approximating function.** Let $p_0(x), p_1(x), \cdots, p_n(x)$ be $n + 1$ functions of x, continuous throughout the interval $a \leqq x \leqq b$, and linearly independent in this interval. Let

$$\phi(x) = c_0 p_0(x) + c_1 p_1(x) + \cdots + c_n p_n(x)$$

be an arbitrary linear combination of these functions with constant coefficients, and let H be the maximum of $|\phi(x)|$ in (a, b).

* Presented to the Society, September 8, 1920.

† D. Jackson, *On functions of closest approximation*, these Transactions, vol. 22 (1921), pp. 117–128. The main problem of the paper cited, going somewhat beyond the result quoted here, had previously been treated, for the polynomial case, by Pólya, in a note with which I was not acquainted at the time of writing: *Sur un algorithme*, etc., Comptes Rendus, vol. 157 (1913), pp. 840–843.

‡ The limitation is in the fact, not merely in the proof. For example, if $f(x) = 1$, $\phi(x) = cx$, in the interval $-1 \leqq x \leqq 1$, the integral of $|f - \phi|$ takes on its minimum value for any value of the coefficient c in the interval $-1 \leqq c \leqq 1$. Here ϕ is still a polynomial, to be sure, but not an arbitrary polynomial of its degree. The coefficients for the best polynomial of the form $c_0 + c_1 x$ are evidently uniquely determined, namely $c_0 = 1, c_1 = 0$.

Then there exists a constant P, completely determined by the system of functions $p_0(x), \cdots, p_n(x)$, such that

$$|c_k| \leqq PH \qquad (k = 0, 1, \cdots, n)$$

for all functions $\phi(x)$.

This lemma, due originally to Sibirani, is proved in the paper already cited,* and the proof need not be repeated here.

Let

$$G = \int_a^b |\phi(x)|\,dx;$$

then there exists a constant Q, completely determined by the system of functions† $p_0(x), \cdots, p_n(x)$, such that

$$|c_k| \leqq QG \qquad (k = 0, 1, \cdots, n),$$

for all functions $\phi(x)$. For‡

$$\left|c_0 \int_a^x p_0(x)\,dx + c_1 \int_a^x p_1(x)\,dx + \cdots + c_n \int_a^x p_n(x)\,dx\right|$$

$$= \left|\int_a^x \phi(x)\,dx\right| \leqq \int_a^x |\phi(x)|\,dx \leqq \int_a^b |\phi(x)|\,dx = G,$$

and it suffices to apply the lemma previously stated to the set of linearly independent functions

$$\int_a^x p_0(x)\,dx, \cdots, \int_a^x p_n(x)\,dx,$$

the constant in this case being denoted by Q.

Finally, let $f(x)$ be a function continuous for $a \leqq x \leqq b$, arbitrary at the outset, but to be kept unchanged throughout the remainder of the discussion; let M be the maximum of $|f(x)|$ in (a, b); let

$$g = \int_a^b |f(x) - \phi(x)|\,dx;$$

and let $\Delta = b - a$. Then, for all functions $\phi(x)$,

$$|c_k| \leqq Q(g + M\Delta),$$

* Loc. cit., Lemma I; the notation has been changed somewhat.

† It is understood that the definition of the functions includes a specification of the interval in which they are defined; when the p's are the successive powers of x, for example, the value of Q will depend on the interval in which they are considered.

‡ Cf. loc. cit., proof of Lemma II.

where Q has the same value as before. For

$$|\phi(x)| \leqq |f(x) - \phi(x)| + |f(x)|,$$

$$\int_a^b |\phi(x)|dx \leqq g + \int_a^b |f(x)|dx \leqq g + M\Delta,$$

and the preceding lemma is applicable.

From this third lemma it follows that if a function $\phi(x)$ is sought to make the value of g as small as possible, all the coefficients $c_0, \cdots, c_n$ that come into consideration belong to a bounded region in the corresponding space of $n+1$ dimensions, a region which may be regarded as closed. As g is a continuous function of the coefficients, there will surely be at least one determination of ϕ for which g actually attains its lower limit γ. Such a function ϕ will be called for brevity an *approximating function*.

3. **Necessary condition for the existence of two approximating functions.** Suppose there are two functions,* $\phi_0(x)$ and $\phi_1(x)$, linear combinations of the p's, for each of which g has the minimum value γ. Let

$$\phi_2(x) = \frac{1}{2}[\phi_0(x) + \phi_1(x)],$$

and let

$$r_i(x) = f(x) - \phi_i(x) \qquad (i = 0, 1, 2).$$

Then

$$r_2(x) = \frac{1}{2}[r_0(x) + r_1(x)].$$

Hence

$$|r_2(x)| \leqq \frac{1}{2}[|r_0(x)| + |r_1(x)|],$$

the sign of equality holding, for any particular value of x, if $r_0 r_1 \geqq 0$, while the relation is an inequality if r_0 and r_1 have opposite signs. If the inequality were to hold for any value of x, it would hold throughout an interval, because of the continuity of the functions, and it would follow that

$$\int_a^b |r_2(x)|dx < \gamma,$$

which is impossible. Consequently either of the remainder functions $r_0(x)$, $r_1(x)$, must be positive or zero at every point where the other is positive, and negative or zero at every point where the other is negative.

* In the earlier paper that has been cited, $\phi_m(x)$ denoted the function for which the integral of the mth power of the absolute value of the error is a minimum. Here the exponent is restricted to the value 1, and the subscript is used without any such special significance.

Suppose there are two points x_1, x_2, in the interval (a, b), such that

$$r_0(x_1) < 0, \qquad r_0(x_2) > 0.$$

Then

$$r_1(x_1) \leqq 0, \qquad r_1(x_2) \geqq 0.$$

There must be at least one point in the interval (x_1, x_2) at which r_0 vanishes, and there must be at least one point where r_1 vanishes. It is to be shown that there must be at least one point where both remainders vanish simultaneously. Let x_1' be the upper limit of the values of x in (x_1, x_2) for which $r_0(x) < 0$, and x_2' the lower limit of the values of x in (x_1', x_2) for which $r_0(x) > 0$. Then $r_0(x)$ is identically zero for $x_1' \leqq x \leqq x_2'$, is negative for points immediately at the left of x_1', and is positive for points immediately at the right of x_2'. For definiteness, and to cover the less obvious case, it will be assumed that $x_1' < x_2'$. If $x_1' = x_2'$, so that the interval reduces to a point, the discussion is essentially the same, though a little simpler. In the interval $x_1' \leqq x \leqq x_2'$, the function $r_1(x)$, being continuous, must either vanish somewhere, or be positive everywhere, or be negative everywhere. But if it were positive throughout the interval, it would be positive, in particular, at the point x_1', and so, by continuity, would be positive at points immediately at the left of x_1', where $r_0(x)$ is negative, and this is inadmissible. Similarly the hypothesis that $r_1(x) < 0$ everywhere has to be rejected. It is certain, then, that $r_1(x)$ must vanish at some point of the interval in question. *In every interval where one of the remainders changes sign, there is at least one point where both remainders vanish simultaneously. At such a point, ϕ_0 and ϕ_1, being both equal to f, are equal to each other.*

To draw further consequences from the relation $r_0 r_1 \geqq 0$, let

$$\phi_t(x) = \phi_0 + t(\phi_1 - \phi_0), \qquad r_t(x) = f(x) - \phi_t(x), \qquad 0 \leqq t \leqq 1.$$

The function previously denoted by $\phi_2(x)$, for example, now has the representation $\phi_{\frac{1}{2}}(x)$. It will always be true that

$$|r_t(x)| = (1 - t)|r_0(x)| + t|r_1(x)|,$$

and therefore

$$\int_a^b |r_t(x)|\,dx = \gamma.$$

Everything that has been said about the pair of functions ϕ_0, ϕ_1, can be said with equal force about the pair of functions ϕ_t corresponding to any two values of t in the interval $(0, 1)$.

4. **Uniqueness of the approximating polynomial.** From now on the generality of the discussion will be restricted, and it will be assumed that

$$p_k(x) = x^k \qquad (k = 0, 1, \cdots, n),$$

so that $\phi(x)$ is a polynomial of the nth degree or lower. In other respects the previous notation will be retained, and it is to be shown that the hypothesis of the existence of two distinct polynomials of approximation, ϕ_0 and ϕ_1, leads to a contradiction.

There are two cases to be distinguished.* Suppose first that $r_0(x)$ changes sign $n+1$ times or more in (a, b). By the italics of the preceding section there must then be at least $n+1$ points where r_0 and r_1 vanish simultaneously, and so at least $n+1$ points where ϕ_0 and ϕ_1 are equal to each other. The identity of the two polynomials follows immediately. If there is any value of t in $(0, 1)$ such that $r_t(x)$ changes sign $n+1$ times or more, the same conclusion can be drawn.

Otherwise, suppose that $r_t(x)$ never changes sign more than n times. For any particular value of t, let $r_t(x)$ change sign just q times, $q \leqq n$. It will be possible to select q points, $x_1, x_2, \cdots, x_q$, so that $r_t(x)$ will be of constant sign (wherever different from zero) in each of the intervals $a \leqq x \leqq x_1$, $x_1 \leqq x \leqq x_2, \cdots, x_q \leqq x \leqq b$, and will take on opposite signs in successive intervals. Let

$$\psi(x) = A(x - x_1)(x - x_2)\cdots(x - x_q),$$

the constant multiplier A being chosen so that the maximum of $|\psi(x)|$ in (a, b) is 1, and so that $\psi(x)$ has the same sign as $r_t(x)$ at some point where $r_t(x) \neq 0$. Then $\psi(x)$ will have the same sign as $r_t(x)$ at every point where $r_t(x)$ is different from zero. If r_t does not change sign at all, it will be understood that $\psi = \pm 1$.

Let ϵ be any positive quantity, and let R_1 be the set of points in (a, b) at which $|r_t(x)| \geqq \epsilon$, S_1 the complementary set, where $|r_t(x)| < \epsilon$. Then, in R_1,

$$|r_t(x) - \epsilon\psi(x)| = |r_t(x)| - \epsilon|\psi(x)|,$$

since r_t and ψ have the same sign, and $|r_t| \geqq \epsilon \geqq \epsilon|\psi|$. In S_1,

$$|r_t(x) - \epsilon\psi(x)| \leqq |r_t(x)| + \epsilon|\psi(x)|.$$

Hence

$$\int_a^b |r_t(x) - \epsilon\psi(x)|\,dx = \int_{R_1} + \int_{S_1} \leqq \int_a^b |r_t(x)|\,dx - \epsilon\int_{R_1} |\psi(x)|\,dx + \epsilon\int_{S_1} |\psi(x)|\,dx,$$

* If it were a question of the integral of the mth power of the absolute value of the error, $m > 1$, the remainder for the approximating polynomial, if not identically zero, would necessarily change sign at least $n+1$ times; cf. loc. cit., end of § 7, noticing that the polynomial there is of degree $n-1$ at most. For $m = 1$, however, it is readily seen that there are other possibilities.

so that

$$\int_a^b |r_t(x) - \epsilon\psi(x)|dx < \int_a^b |r_t(x)|dx$$

unless

$$\int_{S_1} |\psi(x)|dx \geqq \int_{R_1} |\psi(x)|dx.$$

That is, the last relation must necessarily be satisfied, since otherwise the polynomial

$$\phi_t(x) + \epsilon\psi(x)$$

would give a better approximation, in the sense of the integral of the absolute value of the error, than $\phi_t(x)$, which is contrary to hypothesis.

As ϵ is arbitrarily small, it follows further that if R is the set of points where $|r_t(x)| > 0$, and S the complementary set where $r_t(x) = 0$,

$$\int_S |\psi(x)|dx \geqq \int_R |\psi(x)|dx,$$

or, what amounts to the same thing,

$$\int_S |\psi(x)|dx \geqq \frac{1}{2}\int_a^b |\psi(x)|dx. \tag{1}$$

In detail, the argument is as follows: Let $\epsilon_1, \epsilon_2, \cdots$, be a diminishing sequence of positive quantities approaching zero, and let R_j and S_j be the sets corresponding to ϵ_j, after the manner of the preceding paragraph. Then* R is the sum of all the sets R_j, each of which is included in the following, and S is the product of all the sets S_j, each of which is included in the preceding, and therefore

$$\lim_{j=\infty} mR_j = mR, \qquad \lim_{j=\infty} mS_j = mS,$$

the symbol m denoting *measure of*. As

$$\int_R = \int_{R_j} + \int_{R-R_j} \qquad \int_S = \int_{S_j} - \int_{S_j-S},$$

and $\lim_{j=\infty} m(R - R_j) = \lim_{j=\infty} m(S_j - S) = 0$, the desired relation follows immediately.

From (1) it can be inferred that

$$mS \geqq h,$$

where h is a positive quantity depending only on n, a, and b, and independent

* It is convenient to use the language of the theory of Lebesgue integrals, though the problems of measure involved are very simple, since all the functions concerned are continuous, and each point-set that comes into consideration is made up of a finite number or an enumerable infinity of non-overlapping intervals and points.

of the coefficients in the particular polynomial ψ. For, let $\psi(x)$ be any polynomial of degree not higher than n, and let

$$\int_a^b |\psi(x)|dx = G.$$

Then, for each coefficient c_k in ψ,

$$|c_k| \leqq QG,$$

where Q is the constant of § 2. If W is the greatest value of any of the quantities $1, |x|, \cdots, |x^n|$ in (a, b),

$$|\psi(x)| \leqq (n+1)QGW,$$

and for any measurable set S in (a, b),

$$\int_S |\psi(x)|dx \leqq (n+1)QGWmS.$$

Hence (1) implies that*

$$(n+1)QGWmS \geqq \frac{1}{2}G,$$

$$mS \geqq \frac{1}{2(n+1)QW},$$

and the last quantity may be taken as h.

For every value of t in $(0, 1)$, then, it has been proved that $f(x)$ must be identical with $\phi_t(x)$ throughout a point-set of measure at least h. But this is impossible. For the sets S corresponding to two different values of t can not have more than n points in common, since a common point is a point where the two polynomials $\phi_t(x)$ are equal, and hence the measure of the sum of the sets is the sum of their measures; and the necessary condition cannot be satisfied for more than N values of t, where N is the greatest integer contained in $(b-a)/h$. So the desired contradiction has been obtained, and the uniqueness of the approximating polynomial is assured.

It may be emphasized once more that there is no assertion that the remainder for the polynomial of approximation must necessarily change sign $n+1$ times; it must *either* change sign $n+1$ times, *or* vanish identically throughout a finite number or an enumerable infinity of intervals, having at least a certain specified aggregate length.

THE UNIVERSITY OF MINNESOTA,
MINNEAPOLIS, MINN.

* It may be assumed that $g \neq 0$, since there is no occasion for considering a function ψ that vanishes identically.

ON CERTAIN NUMERICAL INVARIANTS OF ALGEBRAIC VARIETIES WITH APPLICATION TO ABELIAN VARIETIES*

BY

SOLOMON LEFSCHETZ

CONTENTS

Number

Introduction.

Part I. PRELIMINARY THEORY.

Chapter I. Cycles and integrals of algebraic varieties.

§1. Some theorems of Analysis Situs 1
2. Effective and algebraic cycles 5
3. Integrals of the second kind 12
4. Periods of integrals of the first kind 15

Chapter II. Invariants ρ and σ of algebraic varieties.

§1. Poincaré's normal functions for algebraic surfaces 17
2. Algebraic cycles of a surface. Fundamental theorem 19
3. Extension to any V_d 29
4. Some applications 38
5. Varieties representing the groups of points of other varieties 44

Part II. ABELIAN VARIETIES.

Chapter I. General properties.

§1. A summary of some fundamental theorems and definitions 46
2. Connectivity of varieties of rank one 52
3. Intermediary functions 57
4. Relation $\rho = 1 + k$. Theorem of Appell-Humbert 69
5. Formulas for the arithmetic genera 75

Chapter II. Abelian varieties with complex multiplication.

§1. Generalities 77
2. Complex multiplication with irreducible characteristic equation 85
3. The characteristic equation is irreducible and Abelian 90
4. Characteristic equation of type $[f(\alpha)]^r = 0, r > 1$. (*a*) Generalities 95
5. Characteristic equation of type $[f(\alpha)]^r = 0$. (*b*) Two important special cases 102
6. Pure matrices of genus two or three 112

Chapter III. Abelian varieties with cyclic group and varieties of rank > 1; images of their involutions.

§1. Varieties of rank one with cyclic group 118
2. Multiple points of Abelian varieties of rank > 1 121
3. Connectivity of varieties of rank > 1 123
4. Integrals of the first kind. Invariants $[\rho]$, ρ, ρ_0^2 127

* Presented to the Society November 27, 1920. This is a translation with minor modifications of the memoir awarded the Bordin Prize by the Paris Academy of Sciences for the year 1919. The publication has been assisted by grants from the American Association for the Advancement of Science and the University of Kansas.

Chapter IV. A class of algebraic curves with cyclic group and their Jacobi varieties.
§1. Integrals of the first kind of the curves $y^q = \Pi_{i=1}^{r+2}(x - a_i)^{a_i}$ (q odd prime) ... 131
2. Curves with three critical points ... 145
3. Curves with four critical points ... 158
4. Curves with $r + 2 > 4$ critical points ... 167

Introduction

In the development of the theory of algebraic functions of one variable the introduction by Riemann of the surfaces that bear his name has played a well-known part. Owing to the partial failure of space intuition with the increase in dimensionality, the introduction of similar ideas into the field of algebraic functions of several variables has been of necessity slow. It was first done by Emile Picard, whose work along this line will remain a classic. A little later came the capital writings of Poincaré in which he laid down the foundations of Analysis Situs, thus providing the needed tools to obviate the failure of space intuition.

Meanwhile other phases of the theory were investigated in Italy and to some extent also in France, receiving an especially powerful impetus at the hands of Castelnuovo, Enriques and Severi. It is however a rather remarkable fact that in their work topological considerations are all but absent, practically never going beyond the study of linear cycles, and this on the whole by very indirect methods. The reason is to be found of course in the fact that the investigations of the Italian School all center around linear systems and the problems that they naturally suggest.

It seems certain that a further use of topological considerations will bring many new results.* In such a development the notion of *algebraic cycles*, or cycles homologous to those formed by algebraic varieties, is destined to play an important part. It is in fact the central concept dominating the first half of this memoir.

After some general theorems on the analysis situs of algebraic varieties and on their multiple integrals, we concentrate our attention on surfaces, where, as could be expected, the results are most expressive. It is found first that a double integral of the first kind has no periods relatively to algebraic cycles, that is, to cycles homologous to those formed by algebraic curves. This result is then inverted by means of certain functions introduced by Poincaré. It follows that Picard's number ρ is equal to the number of two-cycles without periods for the integrals of the first kind, while Severi's number σ is the number of cycles whose multiple is homologous to zero. For higher varieties the result obtained is less precise, ρ being merely at most equal to the number of

*In a monograph entitled *L'Analysis Situs et la Géométrie Algébrique* in course of publication in the Borel Series (Paris, Gauthiers-Villars), I have undertaken a thorough and systematic study of the topology of algebraic surfaces and varieties. Many new and interesting results, discovered since this memoir was written, will be found there. (Added in 1922).

cycles without periods for the double integrals of the first kind. These general theorems are followed by various applications to the determination of ρ and σ in many interesting cases. We may mention in particular what seems to be the first complete proof of a theorem first considered by Noether, to the effect that an arbitrary algebraic surface of order greater than three in ordinary space, possesses only curves that are complete intersections.

The second and main part of this work is entirely devoted to Abelian varieties. Let V_p be such a variety, of rank one and genus p,

$$\Omega \equiv \| \omega_{j\mu} \| \qquad (j = 1, 2, \cdots, p;\ \mu = 1, 2, \cdots, 2p)$$

its period matrix. There exist in general $1 + k$ linearly independent alternate forms with rational coefficients,

$$\sum c_{\mu\nu} x_\mu y_\nu \qquad (c_{\mu\nu} = -c_{\nu\mu}), \tag{1}$$

which vanish when the (x)'s and the (y)'s are replaced by the elements of any two rows of Ω. In particular if a certain inequality due to Riemann is also satisfied, (1) is said to be a principal form of Ω. Instead of the forms (1) we may consider others analogous to them, but no longer constrained to being alternate. The number of linearly independent forms of this more general type will be denoted by $1 + h$ and we always have $h \geqq k \geqq 0$. The properties of matrices such as Ω have recently been the object of searching investigations by Scorza and Rosati.

Now it is found at once that V_p possesses exactly $1 + k$ two-cycles without periods with respect to the integrals of the first kind, and hence for V_p, $\rho \leqq 1 + k$. On the other hand let $\phi(u_1, u_2, \cdots, u_p)$ be an intermediary function

$$\phi(u + \omega_\mu) = e^{-2\pi i(\sum_{(j)} \alpha_{j\mu} u_j + \beta_j)} \cdot \phi(u)$$

the relations which express its behavior relatively to Ω. By considering the effect of adding the (ω_μ)'s followed by the (ω_ν)'s and then reversing the order we obtain at once $\sum_{(j)} (\alpha_{j\mu}\, \omega_{j\nu} - \alpha_{j\nu}\, \omega_{j\mu}) = m_{\mu\nu} = -m_{\nu\mu}$ the (m)'s being integers. We thus have corresponding to ϕ a certain alternate form with integral coefficients

$$\sum m_{\mu\nu} x_\mu y_\nu . \tag{2}$$

On the other hand $\phi = 0$ determines a certain algebraic hypersurface of V_p, and the intersection of $p - 1$ hypersurfaces of the same system is a certain algebraic curve. By evaluating the cycle formed by this curve in terms of a certain simple fundamental system of cycles and then applying Riemann's inequality to the curve, we succeed in showing that the inverse of (2) is a certain principal form of Ω whence follows readily enough $\rho \geqq 1 + k$,

and therefore finally $\rho = 1 + k$. Thus the result obtained in the first part for algebraic surfaces holds for Abelian varieties. All this is to be compared with certain investigations of Appell, Humbert, Bagnera and de Franchis, leading in a wholly different manner to the same conclusion for $p = 2$. There are also some related memoirs by Poincaré.

The consideration of Abelian varieties possessing certain complex multiplications leads us to the determination of h, k, ρ in a wide range of cases. We touch here in many points investigations of Scorza, Rosati, and Frobenius, our methods being more nearly related to those of the last-named author. In the simplest type examined

$$\Omega \equiv || 1, \alpha_j, \alpha_j^2, \cdots, \alpha_j^{2p-1} || \qquad (j = 1, 2, \cdots, p),$$

where the (α)'s together with their conjugates form the roots of an irreducible equation of degree $2p$ with integer coefficients. The determination of h, k, ρ, is shown to be closely related to certain properties of the group of the equation. In particular if this group is Abelian it is shown that in general

$$1 + h = 2(1 + k) = 2\rho = 2p,$$

and V_p does not contain any Abelian subvariety of genus $< p$.

After considering some new properties of Abelian varieties of rank > 1, we pass to the study of the curves

$$y^q = \prod_{(i)} (x - a_i), \qquad (q \text{ odd prime})$$

and of their Jacobi varieties with which the memoir terminates. We have succeeded in determining the total group of birational transformations when the (a)'s are arbitrary. In particular we have showed that in some well-defined cases there are no systems of reducible integrals, that the group is of order q and that the invariants of the Jacobi variety are given by

$$1 + h = 2(1 + k) = 2\rho = 2(q - 1).$$

A remarkable class of curves met with occurs when $q - 1$ is divisible by three. They are birationally transformable to the form

$$x^m y^n + y^m z^n + z^m x^n = 0 \qquad (m^2 - mn + n^2 = q).$$

Their group is a collineation group of order $3q$ if $q > 7$. For $q = 7$, we deal with the famous Klein quartic $x^3 y + y^3 z + z^3 x = 0$, whose group as shown by Klein is the classical simple collineation group of order 168. In all cases we have for the Jacobi varieties $1 + h = 2(1 + k) = 2\rho = 6p = 3(q - 1)$, and there are systems of reducible integrals of genus $(1/3)p$. Special cases have been considered by various authors (Klein, Ciani, Snyder, Scorza).

PART I

PRELIMINARY THEORY

CHAPTER 1. CYCLES AND INTEGRALS OF ALGEBRAIC VARIETIES

§ 1. Some theorems of analysis situs

1. We collect here some notations to be used frequently in the sequence.

V_d, fundamental d-dimensional variety;

S_d, d-space;

$\{C_u\}$, linear pencil depending upon the parameter u and generic in a linear system $|C|$ of hypersurfaces of V_d;

R_i, ith connectivity index of V_d;

$M\,N\cdots P$, intersection of the varieties $M, N, \cdots, P$.

$[M]$, arithmetic genus of M, the number of points of the group when M is a group of points.

In general we shall denote indifferently by M an algebraic variety or its Riemann-image. At times we shall find it convenient to distinguish between them; and then we shall denote the image by (M). Finally by hypersurface of V_d is to be understood a $(d-1)$-dimensional algebraic variety contained in it.

2. Let V_d be an algebraic variety with ordinary singularities, $|C|$ an irreducible linear system, ∞^d at least, without base points, contained in V_d, and such that no point of V_d is multiple for any C through it. Taking then a pencil $\{C_u\}$ we mark in the complex u plane the *critical* points $a_1, a_2, \cdots, a_n$, or points where C_u acquires a conical node and trace cuts $a_0\,a_i$. For the sake of simplification we shall denote the hypersurfaces C_{a_0}, C_{a_i} by C_0, C_i. We propose to prove the following three propositions:

(a) Any i-cycle of $V_d\,(i<d)$ is homologous to a cycle wholly within a C, and when $i<d-1$, the two cycles bound at the same time in their respective manifolds.

(b) Any d-cycle is the sum of two others of which one is wholly within a C and the other is composed of a d-dimensional manifold contained in C_0 plus the loci of certain $(d-1)$-cycles of C_u when u describes the lines $a_0\,a_i$.

(c) The ith connectivity indices, $i\leqq d-2$, of V_d and C are equal.

For linear cycles (a) and (c) have already been proved by Picard, Castelnuovo, and Enriques, for two-cycles of algebraic surfaces by Poincaré, whose method adapted to the general case shall be used here.* We shall also apply his notations $\equiv$, ∞, and say with him: "A is homologous to B (or $A\infty B$), modulo M", to indicate that $A-B$ bounds in M.

*Journal de mathématiques pures et appliquées, ser. 6, vol. 2 (1906), p. 157. See also the writer's paper in the Annals of Mathematics, vol. 21 (1920) as well as the monograph already referred to.

3. Since the propositions to be proved are true for $d = 2$ we can assume that they hold for a V_{d-1} and prove them for a V_d. Any i-cycle of C_u $(i \leqq d-2)$ is homologous to a cycle contained in the base manifold B of $\{C_u\}$. The deformation of the cycle in B must be continuous when u varies, hence it remains homologous to itself, which shows that *any cycle of less than* $(d-1)$ *dimensions of* C_u *is invariant when* u *varies.* Even if the cycle has more than $(d-2)$ dimensions this still applies when it is homologous to a cycle in B.

Let then K_u be the $(2d-1)$-dimensional locus of C_u when u describes the semi-straight line: *argument* $(u - a_0) = Const.$ The manifold K_u cuts an i-cycle Γ_i $(i \leqq d)$ in a certain $(i-1)$-dimensional manifold. By considering the homeomorphism which exists between C_u and C_0 when the above semi-straight line does not contain any critical point, we may show that the $(i-1)$-cycle just considered is homologous to a cycle in C_0. Hence by a slight change in Poincaré's reasoning (loc. cit.) we can show that the cycle Γ_i is homologous to a sum of cycles situated in the hypersurfaces C_k plus a cycle Γ_i' obtained as follows: a certain cycle γ_{i-1}^k of C_u, (u is assumed on $a_0 a_k$), reduced to a point for $u = a_k$, has for locus when u describes the line $a_0 a_k$ a manifold Δ_i^k whose boundary is the position of γ_{i-1}^k in C_0. The cycle Γ_i' is the sum of $\sum \lambda_k \Delta_i^k$ and a manifold Δ_i situated wholly in C_0. According to a remark made above no cycle of less than $(d-1)$ dimensions of C_u disappears at the critical points, hence if $i < d$, Γ_i is homologous to a sum of cycles situated in several (C_u)'s. But when C_u is displaced it can neither gain nor lose cycles of V_d. Hence the cycles situated in several (C_u)'s are all homologous to cycles within one of them, for example C_0. This completes the proof for the first part of (a).

In the case of a d-cycle Γ_d, besides the cycle in C_0 there is the cycle $\sum \lambda_k \Delta_d^k + \Delta_d$ which proves (b). Let now $\Gamma_i \sim 0$ $(i \leqq d-2)$ and denote by M_{i+1} a manifold bounded by Γ_i. By considering the intersections of M_{i+1} and Γ_i with K_u we can show that there is a manifold M_{i+1}', bounded by the cycle Γ_{i+1}' of C_0, to which Γ_i' has been reduced. The manifold M_{i+1}' will be the sum of a manifold in C_0 and of another locus of certain i-cycles of C_u when u describes the cuts. Just as before, since no cycles of less than $(d-1)$ dimensions disappear at the critical points, the part of M_{i+1}' exterior to C_0 can be suppressed. The cycle Γ_{i+1}' will therefore form the boundary for a manifold wholly in C_0. This completes the proof of (a).

4. Let Γ_{i-2} $(i \leqq d+1)$ be an invariant $(i-2)$-cycle of C_u. It will be an arbitrary cycle of C_u for $i < d+1$. Associated with the complex u plane it will generate an i-dimensional manifold Γ_i bounded by the locus of Γ_{i-2} when u describes the cuts. But the parts of this boundary generated by Γ_{i-2} when u describes the opposite borders of the same cut destroy each other, hence Γ_i is an i-cycle. It is besides evident that if $\Gamma_i \sim 0$, also $\Gamma_{i-2} \sim 0$ mod.

C_u. Conversely, if Γ_{i-2} bounds an $(i-1)$-dimensional manifold on C_u, Γ_i bounds its $(i+1)$-dimensional locus when u describes the complex u plane. There might be doubt only if $i-2=d-2$, for then parts of the locus corresponding to the cuts might also have to be considered as forming part of the boundary of the $(i+1)$-dimensional manifold. But in that case we replace Γ_{d-2} by a homologous cycle in CC_u, (C fixed). This amounts to replacing V_d by C for which the difficulty does not present itself any more. A certain cycle $\sim \Gamma_i$ will then bound in C and therefore also in V_d. In this manner R_{d-1} independent cycles of V_d in C_u generate R_{d-1} independent $(d+1)$ cycles of V_d, and as $R_{d-1}=R_{d+1}$, (Poincaré, loc. cit.), every $(d+1)$-cycle depends upon those so obtained. Let us start then with a Γ_{d-i} of V_d in a C^i. It yields first a Γ_{d-i+2} in a C^{i-1}, which in its turn yields a Γ_{d-i+4} in a C^{i-2} etc., so that ultimately we arrive at a Γ_{d+i} of V_d of which Γ_{d-i} is the trace on C^i, and if a multiple of one of the cycles is ~ 0, then also a multiple of the other is ~ 0. Owing to Poincaré's relation $R_{d-i}=R_{d+i}$, every $(d+i)$-cycle depends upon those thus obtained or conversely all $(d-i)$-cycles of V_d in C^i are dependent upon the traces of its $(d+i)$-cycles. Now a $(d-i)$-cycle in C^i can just as well be considered as the trace of a $(d+i-2)$-cycle in a C passing through C^i, and all $(d-i)$-cycles of C^i depend upon the traces of these $(d+i-2)$-cycles of C. The reverse is true, namely, all the $(d+i-2)$-cycles of C depend upon the cycles generated by the $(d-i)$-cycles in the (C^i)'s. It follows that the index R_{d+i-2} of C is equal to R_{d+i}, or, owing to Poincaré's relations, as applied to C, the indices R_{d-i} of both manifolds are equal. This proves (c).

§ 2. Effective and algebraic cycles

5. It is important to distinguish between the cycles which do and those which do not intersect a given hypersurface C. If we merely limit our considerations to an assigned cycle or hypersurface we can not go very far, for the one can be deformed and the other displaced in its continuous system, their intersection thereby being changed. To arrive at a valuable concept we must compare a continuous system of hypersurfaces to a set of homologous cycles. We shall say by definition that an i-cycle Γ_i is *effective* relatively to the hypersurface C if there is a homologous cycle having no point of intersection with a hypersurface of the same continuous system as C.

Let then $|C|$ be a linear system such as we have already considered, and assume that a cycle $\Gamma_i\,(i \leqq d)$ meets a C along a Γ_{i-2}.

In the intersection CC_1 of C with another hypersurface C_1 of the system there exists, (No. 2), a Γ'_{i-2} trace of a cycle Γ''_i of C, $\sim$ mod. C to a multiple of Γ_{i-2}. Replacing if necessary Γ_i by an adequate multiple, we may say that $\Gamma'_{i-2} \sim \Gamma_{i-2}$ mod. C. Now make C_1 tend towards C in $|C|$, while main-

taining $|CC_1|$ and Γ'_{i-2} fixed. Γ'_i will tend towards a cycle Γ'_i of C_1, whose trace on CC_1 will still be Γ'_{i-2}. We thus have a cycle Γ'_i of C_1, whose trace on CC_1 bounds with Γ_{i-2} a certain M_{i-1} of C.

Let now E_2 be a two-dimensional elementary sensed manifold or "element" passing through a point A of C and transverse to C. Together with a sensed $(2d-2)$-fold element of C through A it determines the sensing of V_d, and since C and V_d are both two sided, when A describes any closed path in C, E_2 may be displaced at the same time without ever acquiring a line segment in common with C, so as to return to its former position with sense unchanged. The following analogous occurrence in ordinary space will make this clearer: When the origin A of a directed segment AB describes a closed path on a two-sided surface, AB may be displaced without ever becoming tangent to the surface, so as to return exactly to its original position.

To come back to our question, let A describe M_{i-1} and displace E_2 in the manner just indicated so that moreover when A is in Γ_{i-2} or Γ'_{i-2}, E_2 will be in Γ_i or Γ'_i respectively. In these conditions a circuit surrounding A in E_2 will generate a manifold M_i meeting nowhere C, and if we suppress in $\Gamma_i - \Gamma'_i + M_i$ the part generated by the area of E_2 which is bounded by ζ when A describes Γ_{i-2} or Γ'_{i-2}, we obtain a cycle $\sim (\Gamma_i - \Gamma'_i)$, since we can make it tend towards this cycle as a limit, and this new i-cycle is *effective* relatively to C. But Γ'_i, which is in C_1, is $\sim$ to a cycle wholly in C. Hence, *there exists a combination of any i-cycle $(i \leqq d)$ and of cycles wholly in C, effective with respect to C.*

ALGEBRAIC CYCLES. These cycles, which occur when i is even, are simply the cycles homologous to a combination of those formed by the algebraic manifolds of V_d. The cycles formed by algebraic curves have been considered by Poincaré although he made no application of them.

6. A non-bounding d-cycle of C is also one of V_d, for when C varies in its system it neither gains nor loses $(d-2)$-cycles and therefore d-cycles, so that they are invariant. Hence the number of d-cycles non-effective relatively to C is equal to the dth index of connectivity of the hypersurface, hence also to its $(d-2)$th index and therefore, according to what we have already shown, to R_{d-2}. If we denote by R'_i the number of i-cycles effective with respect to C, we shall have $R'_d = R_d - R_{d-2}$.

Let now $i \leqq d-1$. Any i-cycle of V_d is homologous to a cycle in C^{d-i}. Replacing then V_d by C^{d-i}, which has the same number of effective i-cycles with respect to a C^{d-i+1} as V_d with respect to C, we obtain

$$R_i - R'_i = R_{i-2}, \qquad R_2 - R'_2 = 1 \qquad (2 < i \leqq d).$$

The second formula follows from the fact that we have to take into account the non-effective algebraic cycle C^{d-1}.

In the next chapter it will be shown that on an algebraic surface the algebraic curves are non-effective cycles with respect to a curve in a properly chosen system. Moreover, from the above it follows that if C is a plane section, A any other curve, Γ any two-dimensional cycle, a certain cycle $mA + n\Gamma\,(n \neq 0)$ is effective with respect to C. The proof holds as well if C is generic in a certain linear system $|C|$ analogous to the system of hypersurfaces of similar name. This establishes the second formula for $d = 2$. When $d > 2$, a multiple of any Γ_2 is homologous to a cycle in C, which shows that we may replace V_d by V_{d-1}; hence this second formula holds for all cases.

We thus see that R'_i does not depend upon the special system $|C|$ considered, provided it has certain general properties specified in No. 2.

7. From the formulas obtained follow these:

$$R_{2i} = \sum_{h=0}^{i} R'_{2h}, \qquad 2i \leqq d$$

$$R_{2i+1} = \sum_{h=0}^{i} R'_{2h+1}, \qquad 2i + 1 \leqq d;$$

$$(R'_1 = R_1, \qquad R_0 = 1).$$

Hence if $R_{2i} = 1$, its minimum value, $R'_{2h} = 0, R_{2h} = 1, h \leqq i$, and if $R_{2i+1} = 0$, $R'_{2h+1} = R_{2h+1} = 0$, $h \leqq i$. In particular if a single $R_{2i+1} = 0$, $R_1 = 0$ *and* V_d *is regular.*

Finally let us notice explicitly that a *multiple of an* i*-cycle non-effective with respect to* C *is the sum of an effective cycle and of a cycle in* C^{d-i+1}. For $i = 2$, the multiple of any non-effective cycle is the sum of an effective cycle and the algebraic cycle C^{d-1} taken a certain number of times.

Let us mention here a formula derived first by Alexander* and giving R_d in terms of the (R_i)'s and of the Zeuthen-Segre invariant I_d of V_d. It can be written

$$R_d = I_d + 2\sum_{i=1}^{d-1} (-1)^{d-i+1} R_i + 2(-1)^d (d-1).$$

8. Let $A_1, \cdots, A_s$ be hypersurfaces of V_d and assume $|C|$ so chosen that it contains their sum, leaving a residue $|K|$, linear system of the same type as $|C|$. Let now $C_0 = A_1 + A_2 + \cdots + A_s + K$, and, instead of considering a pencil $\{C_u\}$ generic in $|C|$, let us take one containing C_0. Reasoning in regard to this pencil as previously we find that the multiple of any d-cycle is the sum of a cycle effective with respect to the hypersurfaces A_r, K, and of a cycle contained within one or more of these hypersurfaces, and non-effective with respect to their totality. The number of effective cycles will now be $R'_d - r_d$, $r_d \geqq 0$. Thus there will be r_d cycles effective with respect to K,

*Rendiconti dei Lincei, ser. 5 vol. 23 (1914), pp. 55–62.

but not with respect to the (A)'s. Since $r_d \leqq R'_d$, when any set of hypersurfaces whatever is considered, this integer has a maximum ρ_d which is obviously a numerical invariant of V_d. It is the maximum number of cycles contained in the hypersurfaces of V_d and yet effective with respect to an irreducible linear system, ∞^d at least, without base points.

A similar invariant ρ_i may be defined for i-cycles. The invariants ρ_i of V_d and of C are the same when $i \leqq d-2$. Hence ρ_i is the same for V_d and C^k, $k \leqq d-i-1$. In particular ρ_2 is the same for V_d and C. We shall see that for any V_d, $1+\rho_2$ is equal to Picard's number ρ.

9. *Torsion indices.* It may happen that two i-cycles Γ_i, Γ'_i, without being homologous to each other, are nevertheless such that $\lambda\Gamma_i \sim \lambda\Gamma'_i$, $\lambda > 1$. The cycle $\Delta_i = \Gamma_i - \Gamma'_i$ is called a *zero-divisor*. Poincaré has shown that when this occurs, V_d undergoes a sort of internal torsion and the (λ)'s are related to his so-called *torsion-coefficients*. He further established that the torsion coefficients for i-cycles are equal to those for the $(2d-i-1)$-cycles.

The operations $+\Delta_i$ applied to the i-cycles give rise to an abelian group whose order σ_i is the product of the torsion coefficients. We shall call it the ith *torsion index*. These indices satisfy the relation $\sigma_i = \sigma_{2d-i-1}$, $\sigma_{2d-1} = 1$. In particular, $\sigma_1 = \sigma_{2d-2} = \sigma$ is the invariant of Severi, as we shall see later. That is in an algebraic surface it turns out that the zero divisors for the cycles or algebraic curves lead all to the same numerical invariant. Algebraic surfaces with $\sigma > 1$, of which examples have been given by Severi and Godeaux, have then the property of possessing linear cycles that do not bound, but of which a certain multiple bounds.

Since any i-cycle, $i \leqq d-2$, is homologous to a cycle in C and also since such cycles when in C form cycles of V_d, V_d and C have the same zero divisors for these cycles and therefore *equal invariants* σ_i, $i \leqq d-2$.

10. The notions of *base, intermediary base, minimum base* are commonly useful. Let $A_1, A_2, \cdots$ be a set of entities forming a modulus, i.e., having these properties: (a) The sum or difference of any two belong to the set, (b) the zero of the set is well defined, (c) $A+B$ does not differ from $B+A$. The entities $A_1, \cdots, A_n$ are said to form a *base* if for every A there is a relation $\lambda A = \lambda_1 A_1 + \lambda_2 A_2 + \cdots + \lambda_n A_n$, where the (λ)'s are integers. If λ always divides all the (λ_i)'s the base is called *intermediary*, while if for every A we can take $\lambda = 1$, we have to deal with a *minimum base*. Examples of such systems are given by the i-cycles of a closed manifold, the hypersurfaces of a V_d, etc.

Repeating for the i-cycles a discussion of Severi's* for algebraic curves it can be shown that the i-cycles of V_d possess ordinary and minimum bases composed of R_i and $R_i + \sigma_i - 1$ cycles respectively.

*Annales de l'Ecole Normale supérieure, ser. 2, vol. 25 (1908), pp. 449–468. The nomenclature is his.

11. If V_d possesses arbitrary singularities but is birationally transformable into V'_d, variety with ordinary singularities, the neighborhood of the extraordinary singularities of V_d may be considered as forming a certain number of infinitesimal algebraic varieties. We shall thus be led to consider infinitesimal i-cycles contained in these varieties and corresponding to finite cycles on V_d.

In general an invariant m may take a different value according as infinitesimal cycles are or are not taken into consideration. Reserving the ordinary notation for the first case we shall denote the invariant in the second by $[m]$. This notation has already been used by Bagnera and de Franchis for the number ρ. We shall then have $R_i - [R_i] = \rho_i - [\rho_i]$.

Remark. If V_d has ordinary singularities, in considering the i-cycles contained in a given hypersurface, the infinitesimal cycles must be left out, that is, no attention must be paid to accidental singularities of the hypersurface.

§ 3. Integrals of the second kind

12. Much interest is added to the discussion by introducing integrals of the second kind. The author has recently published a series of results (most of them without proofs) relating to triple integrals of a V_3* and a memoir containing the proofs is ready for publication. In another memoir he has given the extension to double integrals of a V_3†, of the Picard theory of double integrals of the second kind of algebraic surfaces. The extension from $d = 2$ to $d = 3$ presents many difficulties which seem to disappear in the extension from $d = 3$ to any other value of d. We shall then indicate mostly without proofs the statements for a V_d:

Let $F_d(x_1, x_2, \cdots, x_d, t) = 0$ be the equation of V_d still assumed irreducible and with ordinary singularities, $|H|$ the system of hyperplane sections, H_{x_i} the section by $x_i = \text{const}$. The integral

$$(1) \qquad \int\int \cdots \int U(x_1, x_2, \cdots, x_d, t)\, dx_1\, dx_2 \cdots dx_d \quad (U \text{ a rational function}),$$

is of the *second kind* if to every hypersurface of infinity A of U corresponds an integral of type called *improper* of the second kind,

$$(2) \qquad \int\int \cdots \int \sum \frac{\partial U_i}{\partial x_i}\, dx_1\, dx_2 \cdots dx_d \quad (U_i \text{ a rational function}),$$

such that their difference is finite in the neighborhood of an arbitrary point of A. If (1) is not of the type (2) it is said to be *proper* of the second kind.

Proper and improper integrals preserve their character under birational

*Comptes Rendus, vol. 165 (1917), pp. 850–854.

†Annali di matematica, ser. 3, vol. 26 (1917), pp. 227–261.

transformations. The number ρ_0^d of proper integrals of which no linear combination is improper is an absolute invariant. If the system of hyperplane sections is adequately selected every integral of the second kind can be reduced by subtraction of an improper integral to the *normal* form

$$\int\int \cdots \int \frac{P(x_1, x_2, \cdots x_d, t)}{F_t'}\, dx_1\, dx_2 \cdots dx_d, \tag{3}$$

where P is an adjoint polynomial.

Whether of the second kind or not, (3) has *periods* and *residues*, but only relatively to finite cycles or cycles effective relatively to the hypersurface at infinity. Indeed, as Picard has shown, if the cycle is infinite the corresponding value of (3) is indefinite or if definite may vary when the cycle is deformed.

In connection with (3) we may also consider

$$\int\int \cdots \int \frac{P(x_1, x_2, \cdots, x_d, t)}{F_t'}\, dx_1\, dx_2 \cdots dx_{d-1}, \tag{4}$$

attached to H_{x_d}. Its periods satisfy a linear homogeneous differential equation—the equation of Picard-Fuchs. By expressing the periods of (3) in terms of those of (4) we may show that when P is properly chosen they assume an arbitrary value.

13. Let then r_i' be the number corresponding to R_i' for H. On the strength of what has been stated we may derive this formula, in which N denotes the class of V_d, $R_d' = N - 2(r_{d-1}' - R_{d-1}') - (r_{d-2}' - R_{d-2}')$, as being the exact number of integrals without residues, but with some non-zero periods. These integrals are of the second kind and every proper integral is reducible to them.

By means of this relation we may derive Alexander's formula for R_d. Indeed, if I_s is the Zeuthen-Segre invariant of H^{d-s} we have for V_d:

$$I_d = N - 2I_{d-1} - I_{d-2}$$

$$\therefore\quad R_d' - I_d = 2R_{d-1}' + R_{d-2}' - 2(r_{d-1}' + I_{d-1}) - (r_{d-2}' - I_{d-2})$$

and similarly for H^{d-s} $(s = 3, 4, \cdots, d-1)$,

$$r_s' - I_s = 2R_{s-1}' + R_{s-2}' - 2(r_{s-1}' - I_{s-1}) - (r_{s-2}' - I_{s-2}),$$

$$r_2' - I_2 = 2R_1 + 1,$$

whence

$$R_d' = I_d + (-1)^d \cdot (d-1) + \sum_{i=0}^{d-2} (-1)^{d-i} \cdot (d-i) \cdot R_{i+1}',$$

which reduces to Alexander's formula for R_d if we remember that

$$R_i' = R_i - R_{i-2}$$

and set, as we should, $R_0 = 1$, $R_{-1} = 0$.

Let us return to our integral of the second kind under normal form. If its periods are all zero, it is improper of the second kind. We shall show below that there are exactly ρ_d improper integrals with non-zero periods, hence for the number of proper integrals

$$\rho_0' = R_d' - \rho_d = I_d + 2(-1)^d(d-1) - \rho_d + \sum_{i=0}^{d-2}(-1)^{d-i}(R_{i+1} - R_{i-1})$$

$$= I_d + 2(-1)^d(d-1) - \rho_d - R_{d-2} + 2\sum_{i=1}^{d-1}(-1)^{d-i+1}R_i.$$

For $d = 2$ this becomes a well-known formula given by Picard and for $d = 3$ it becomes the formula of the author's Comptes Rendus note, the λ of the note being the same as ρ_d.

14. We will now outline the proof that *there exist ρ_d improper integrals in normal form and with non-zero periods.*

Let then $A_1, A_2, \cdots, A_n$ be hypersurfaces such that there are ρ_d finite cycles $\Gamma_1, \Gamma_2, \cdots, \Gamma_{\rho_d}$ non-effective relatively to some of the (A)'s. We shall assume (as we may) that the simple hypersurface of intersection of $F_t' = 0$ with V_d is among the (A)'s. There are $R_d' - \rho_d$ cycles, $\Gamma_1', \Gamma_2', \cdots, \Gamma_{R_d'-\rho_d}'$, effective relatively to H, or as a special case finite, which do not meet the (A)'s.

It is sufficient to show that from any integral of the second kind in the normal form we may subtract an improper one so that the difference will be without periods relatively to the (Γ)'s. Indeed, by means of a change of variables it can be shown that (4), extended to a closed continuum, where it is finite and where $F_t' \neq 0$, yields a zero period.* It follows that an improper integral under the normal form has no period relatively to the (Γ')'s and therefore the $R_d' - \rho_d$ integrals that may be formed having no periods with respect to the (Γ)'s, but having some with respect to the (Γ')'s, are certainly proper. As by assumption all proper integrals are reducible to them, we must have $\rho_0' = R_d' - \rho_d$. Therefore there must be $\rho_d = R_d' - \rho_0'$ improper integrals in the normal form with non-zero periods.

Let Γ_{ik} be the $(d-2)$-cycle intersection of Γ_i and A_k. A multiple of Γ_{ik} is homologous mod. A_k to a $\overline{\Gamma}_{ik}$ situated in $H_{x_1} A_k$, wherein it is invariant when x_1 varies. Replacing if need be Γ_i by a certain multiple of itself we may assume that actually $\Gamma_{ik} \sim \overline{\Gamma}_{ik}$ mod. A_k. The possible exceptional singularities of A_k need not be taken into account for the theorems of No. 2 are readily seen to hold even then since Γ_{ik} is of dimensionality $d-2$ and Γ_i may be assumed not to go through the exceptional singularities.

By reasoning as in No. 5, we may reduce Γ_i to a cycle cutting A_k in $\overline{\Gamma}_{ik}$ and nowhere else. Henceforth assume that Γ_i is that very cycle, Γ_{ik} thus coinciding with $\overline{\Gamma}_{ik}$. We can then arrange matters so that the vicinity of Γ_{ik}

* The proof for $d = 2$ is given in the author's Annali di matematica paper, no. 8.

in Γ_i be entirely in H_{x_1}. It constitutes a small region bound by a $(d-1)$-cycle Δ_{ik}. Suppress these regions from Γ_i and let M_i be what is left.

We observe that if U_1 is a rational function infinite on the (A)'s only

$$\int\int\cdots\int_{M_i}\frac{\partial U_1}{\partial x_1}\,dx_1\,dx_2\cdots dx_d=\sum\int\int\cdots\int_{\Delta_{ik}}U_1\,dx_2\,dx_3\cdots dx_d$$

$$\int\int\cdots\int_{M_i}\frac{\partial U}{\partial x_{h+1}}\,dx_1\,dx_2\cdots dx_d=0.$$

Thus the first d-uple integral is a sum of residues of

$$\int\int\cdots\int U_1\,dx_2\,dx_3\cdots dx_d, \tag{5}$$

attached to H_{x_1}, relatively to the cycles Γ_{ik}.

It may be shown that the residues at finite distance of (5)* are as arbitrary as if U_1 were no more constrained to be rational in x_1. This follows in principle from the fact that an integral of a rational function belonging to a V_d and with arbitrary residues can be formed by operations rational with respect to the coefficients of its equation.

A corollary is the existence of an integral (5) with constant residues with respect to the cycles such as Γ_{ik}. In that case

$$\frac{\partial}{\partial x_1}\int\int\cdots\int U_1\,dx_2\,dx_3\cdots dx_d \tag{6}$$

behaves like an integral of the second kind at finite distance. From this can be deduced the existence of rational functions $U_2, U_3, \cdots, U_d$, such that

$$\sum_{i=1}^{d}\frac{\partial U_i}{\partial x_i}=\frac{P(x_1, x_2, \cdots, x_d, t)}{\phi(x_1)F_t'}$$

where P is an adjoint polynomial and ϕ an ordinary polynomial. From the relations established above, and since the integral at the left in (7), taken over $\Gamma_i - M_i$, is very small, follows then

$$\int\int\cdots\int_{\Gamma_i}\frac{P\cdot dx_1\,dx_2\cdots dx_d}{\phi\cdot F_t'}=\sum\int\int\cdots\int_{\Delta_{ik}}U_1\,dx_2\,dx_3\cdots dx_d. \tag{7}$$

Hence the period of (7) as to Γ_i, like the residues of (5) as to Γ_{ik}, is completely arbitrary. Thus we may obtain an improper integral of the second kind (7) with arbitrary periods relatively to the (Γ)'s. As (7) may be shown to be reducible to the normal form without gain or loss of periods, we see finally that its periods relatively to the (Γ')'s are zero since these last cycles are effective relatively to the (A)'s. As the periods of (7) relatively

*Quarterly journal of mathematics, vol. 49 (1917), pp. 333–343.

to the (Γ)'s are perfectly arbitrary we may obtain an improper integral in the normal form which when subtracted from a given integral of the second kind in that form will yield one without periods with respect to the (Γ)'s, and this proves our theorem.

All that precedes may be extended to integrals of "total differentials," that is, to integrals of the type $\int\int\cdots\int \sum P_{i_1 i_2 \ldots i_s}\, dx_{i_1}\, dx_{i_2}\cdots dx_{i_s}$, where the (P)'s are rational and satisfy Poincaré's conditions of integrability. For example, when $s = 2$, these conditions are

$$\frac{\partial P_{ik}}{\partial x_l} + \frac{\partial P_{kl}}{\partial x_i} + \frac{\partial P_{li}}{\partial x_k} = 0.$$

The integral will be proper or improper of the second kind according as it determines an integral of one or the other type on an arbitrary H. This makes it possible to define these integrals by recurrence. The number of proper integrals of the second kind is $\rho_0^s = R_s' - \rho_s = R_s - R_{s-2} - \rho_s$.

In particular for $s = 2$ we have $\rho_0^2 = R_2' - \rho_2 = R_2' - (\rho - 1) = R_2 - \rho$. This special case $s = 2$ has already been considered* by the author of the present paper.

§ 4. Periods of integrals of the first kind

15. Integrals of the first kind are defined as usual as those which are everywhere finite. While restrictions were necessary before as to cycles relatively to which integrals of the second kind could properly be assumed to have periods, they cease to be necessary when we deal with integrals of the first kind. However, the question may be asked, *how many of the R_s periods which an s-uple integral of the first kind may have, are linearly independent in the field of rational numbers*, in the sense that they do not have to satisfy a linear homogeneous equation with integral coefficients. Let us assume at first $s = d$ and consider the integral of the first kind

$$\int\int\cdots\int \frac{P(x_1, x_2, \cdots, x_d, t)}{F_t'}\, dx_1\, dx_2 \cdots dx_d. \tag{8}$$

What can be said as to its period relatively to a d-cycle Γ_d non-effective relatively to H? By combining Γ_d with effective cycles we may derive a cycle contained in H_{x_1}. Grant that this has already been done for Γ_d. It will intersect the H^2 at infinity of H_{x_1} in a $(d-2)$-cycle Γ_{d-2}. We may isolate on Γ_d the vicinity of Γ_{d-2}, the boundary of the isolated part Γ_d' being a manifold M_{d-1} — a tube for $d = 3$. The integral (8) extended to $\Gamma_d - \Gamma_d'$ gives zero since $dx_1 = 0$ at all points of this continuum and it is at finite distance. Let us make a projective transformation reducing the H^2 at in-

*Annali di matematica, loc. cit. In the formula there given R_2 should be replaced by R_2' as only finite cycles are considered.

finity of H_{x_1} to $H_{x_1}\, H_{x_2}$. Keeping notations unchanged we see that the period of (8) relatively to Γ_d is equal to the value of (8) extended over Γ'_d, a portion of the cycle near Γ_{d-2}, and this will certainly give zero if

$$\int\int \cdots \int \frac{P(x_1, x_2, \cdots, x_d, t)}{F'_t}\, dx_3\, dx_4 \cdots dx_d \tag{9}$$

has no period relatively to Γ_{d-2}. Now if Γ_{d-2} is finite, that is, if it is effective relatively to H, the period in question is certainly zero. For, maintaining x_1 fixed, we see that the periods of (9) vanish when $x_2 = \infty$ because P is an adjoint canonical polynomial (that is of degree $m - d - 2$, where m is the degree of V_d). But as x_2 varies the period relatively to Γ_{d-2}, cycle of V_d in $H_{x_1}\, H_{x_2}$, is rational in x_2, finite everywhere since the cycle is finite, hence constant and zero at infinity, and therefore identically zero.

The same result can be obtained differently. The doubtful part of Γ_d is composed of $\infty^2\,(d-2)$-cycles differing very little from Γ_{d-2}, and the value of (8) extended over Γ'_d is equal to the constant period of (9) relatively to Γ_{d-2} integrated over a finite two-dimensional continuum of the complex (x_1, x_2) space, and therefore again zero.

We have thus obtained R'_{d-2} d-cycles with respect to which (8) has no periods. The same reasoning may be pursued by replacing (8), V_d and Γ_d by (9), H^2 and Γ_{d-2}, and so on. *We shall have finally*

$$R'_{d-2} + R'_{d-6} + \cdots = R_{d-2} - R_{d-4} + R_{d-6} \cdots$$

non-effective d-cycles relatively to which integrals of the first kind have no periods. Similarly there are $R_{s-2} - R_{s-4} + \cdots$ non-effective s-cycles with respect to which s-uple integrals of the first kind have no periods. In these expressions the last term is either $\pm R_1$ or $\pm R_0 = \pm 1$.

16. It is easy to show that s-tuple integrals of the first kind have no periods relatively to the ρ_s cycles of No. 8. To show this, transform V_d birationally into a variety V''_d with ordinary singularities in such a way that the transformed A'_k of A_k be part of the hyperplane section $x_1 = 0$. The finite cycles contained in the (A'_k)'s will now yield zero for period since at every point of them $dx_1 = 0$. The same is true for finite cycles of V_d that have become infinitesimal on V''_d,—a circumstance that may well happen—, for these infinitesimal cycles may be assumed at finite distance also. Thus *there will be in all $\rho_s + R_{s-2} - R_{s-4} + R_{s-6} \cdots$ distinct s-cycles relatively to which integrals of the first kind have no periods.*

Are there any others with the same property? Probably not, though we have succeeded in proving it only for algebraic surfaces and for abelian varieties with a period matrix as general as possible.

CHAPTER 2. INVARIANTS ρ, σ OF ALGEBRAIC VARIETIES

§ 1. Poincaré's normal functions for algebraic surfaces

17. Let $F(x, y, z) = 0$ represent an algebraic surface V_2, of order m, irregularity $\frac{1}{2}R_1 = q$, and denote by $|H|$ and p the system of plane sections and the genus of a generic H. As is well known, a set of p independent integrals of the first kind of H_y, arbitrary curve of the pencil $\{H_y\}$, can be obtained thus: For the first $p - q$ integrals we take

$$u_h = \int \frac{P_h(x, y, z)\,dx}{F_z'} \qquad (h = 1, 2, \cdots, p - q),$$

where P_h is an adjoint polynomial of order $m - 3$, and for the remaining we take the q integrals of the first kind $u_{p-q+1}, u_{p-q+2}, \cdots, u_p$ of V_2. Let $A_1, A_2, \cdots, A_m$ be the base points of $\{H_y\}$, C any algebraic curve of V_2, $M_1, M_2, \cdots, M_n$ the variable points of the group CH_y or these points associated with some of the (A)'s. Consider the abelian sums

$$v_h(y) = \sum_{j=1}^{n} \int_{A_1}^{M_j} du_h \qquad (h = 1, 2, \cdots, p),$$

first introduced by Poincaré,* who gave for them expressions which the present choice of integrals of the first kind reduces to

$$(1) \qquad v_h(y) = \sum_{k=1}^{N} \frac{\lambda_k}{2\pi i} \int_b^{b_k} \frac{\Omega_{hk}(Y)}{Y - y}\,dY \qquad (h = 1, 2, \cdots, p - q),$$

$$v_{p-q+s} = \beta_s \qquad (s = 1, 2, \cdots, q).$$

In these expressions the (λ)'s are integers, called *characteristic integers*, b arbitrary, $b_1, b_2, \cdots, b_N$ the critical values of y for $\{H_y\}$, the (β)'s constants, and finally Ω_{hk} the period of u_h relatively to the cycle of H_y that vanishes for $y = b_k$. The corresponding periods of u_{p-q+s} are obviously zero. The paths of integration form a system of non-intersecting cuts in the y plane.

In the expressions as given by Poincaré there appear certain rational functions at the right. These expressions can only be polynomials, for their infinities are the same as those of the (u)'s. Moreover, by means of the birational space transformation $x = x'/y'$, $y = 1/y'$, $z = z'/y'$, we may easily verify that $v_h(y)$, $h \leqq p - q$, vanishes at infinity, while the other (v)'s are finite there, hence the form of the expressions (1) follows. Besides it can be shown directly that v_{p-q+s} is constant for it is uniform in y and finite everywhere (Severi).

*Annales de l'Ecole Normale supérieure, ser. 2, vol. 27 (1910), pp. 55–108. Sitzungsberichte der Berliner mathematischen Gesellschaft, vol. 10 (1911), pp. 28–55.

18. We obtain a first set of relations to be satisfied by the quantities entering in the (v)'s when we express the fact that the (v)'s are independent of b or that $\partial v_k/\partial b = 0$.

If in the relation obtained we replace b, which is arbitrary, by y, it becomes

$$\sum_{k=1}^{N} \lambda_k \, \Omega_{hk}(y) = 0 \qquad (h = 1, 2, \cdots, p - q). \tag{2}$$

This condition once satisfied, the (v)'s as given by (1) are regular everywhere, infinity included, except at the critical points b_i, and this is as it should be.

Another condition is obtained thus: Let there be a value $y = \alpha$ for which

$$\sum_{h=1}^{p-q} \frac{\gamma_h \, P_h(x, y, z)}{(y - \alpha)^s}$$

remains finite, the (γ)'s being constants. Then $\sum \gamma_h \, v_h(y) \cdot (y - \alpha)^{-s}$ must also remain finite. We can always select our integrals so that $s = 1$ for all the (α)'s (Poincaré), but this is immaterial.

A set of functions satisfying these two conditions and behaving like the (v)'s at the critical points forms what Poincaré has called a set of *normal functions*. He has proved the following fundamental theorem: *To a set of normal functions always corresponds an algebraic curve for which they are Abelian sums.* Exceptionally, the curve is reduced to one or more of the points A_i.

Given two algebraic curves B, C, of V_2, we will write with Severi $B = C$, if there exists an algebraic curve E such that $B + E$, $C + E$ are both total curves of the same continuous system.* When B varies in its continuous system the characteristic integers corresponding to the total group BH_y are fixed. They are only determined however up to a system of integers corresponding to a period, as the periods obviously form sets of normal functions. The set of characteristic integers of $B + E$ is obtained by adding the corresponding integers of B and E. Hence if $B = C$, the differences between their characteristic integers form a set corresponding to a period, it being understood that characteristic integers are taken for the total groups BH_y, CH_y.

§ 2. Algebraic cycles of a surface. Fundamental theorem

19. We propose first to interpret the conditions that the (v)'s must satisfy from a somewhat different viewpoint.

We begin with the second condition. When $\sum \gamma_h \, P_h(x, y, z) = (y - \alpha) \cdot Q(x, y, z)$, Q is an adjoint polynomial of order $m - 4$ and the double integral,

$$\iint \frac{Q(x, y, z)}{F'_z} \, dxdy \tag{3}$$

*These systems may be reducible but must be connected. A thorough treatment of this point has been given by Albanese, Annali di matematica, ser. 3, vol. 24 (1915), pp. 159-233. Our "equivalence" is the same as his "virtual equivalence".

is of the first kind. Let $\omega_k(y)$ be the period of

$$\int \frac{Q(x, y, z)}{F_z'}\, dx \tag{4}$$

corresponding to Ω_{hk} for u_h. We must have

$$\sum_{h,k} \gamma_h \lambda_k \int_b^{b_k} \frac{\Omega_{hk}(Y)\, dY}{Y - \alpha} = \sum_k \lambda_k \int_b^{b_k} \omega_k(y)\, dy = 0. \tag{5}$$

Conversely if (3) is of the first kind,

$$\int \frac{(y - \alpha) Q(x, y, z)}{F_z'}\, dx$$

is a linear combination of $u_1, u_2, \cdots, u_{p-q}$, identically zero for $y = \alpha$, and the relation (5) corresponding to it must be satisfied. Hence (5) is true whatever the integral of the first kind (3) considered.

20. Let Γ be any two-cycle of V_2. We may assume without loss of generality that any H_y meets it in a finite number of points since this can always be obtained by slightly deforming the cycle if necessary. Since Γ is two sided we may sense it by assigning a positive direction of rotation for its small circuits. Let now y describe a small positive circuit in its plane. Of the points of intersection of Γ and H_y, a certain number, say n', will describe positive circuits on Γ, while the n'' remaining points will do just the opposite. The number $n' - n''$ does not depend upon the position of the circuit in the y plane, for when a point of one type disappears one of the other disappears at the same time. The number $n' - n''$ is therefore a definite simultaneous character of the two manifolds Γ, H_y. Poincaré introduced it for manifolds M_s, M_{k-s} in an M_k (the indices indicate the dimensionality), and he denoted it by $N(M_s\, M_{k-s})$. The N really is superfluous, and we shall simply write $(M_s\, M_{k-s})$, or $(\Gamma\, H_y) = n' - n''$. All we need to know concerning it here is that if $\Gamma \sim 0$, also $(\Gamma\, H_y) = 0$.

We observe at once that if Γ is an algebraic cycle (C), of the two numbers n', n'', one is necessarily zero, the other being equal to $\pm [CH_y]$, or in absolute value equal to the order of C. This follows from the well-known property of a multiply sheeted Riemann surface, that when the independent variable describes a small circuit in its plane, the corresponding points in the various sheets describe circuits sensed alike relatively to the surface. We shall make once for all the convention that (C) is to be so sensed that $(C\, H_y) = [CH_y]$.

Returning to the cycle Γ, let us join A_1 to all the points of intersection of Γ and H_y by lines in H_y. Their locus as y describes its plane without crossing the cuts bb_k is a manifold M_3 whose boundary is composed of Γ, of part or all of H_y, and of a manifold M_2 that may be described thus: When y goes from

y_0 on one side of bb_k to the point y_0' right opposite on the other, by turning around b_k without crossing the cut, the aggregate of lines whose locus is M_3 returns to a new position in $H_{y_0} = H_{y_0'}$, which differs from the old position by a multiple of the linear cycle δ_k of H_y that reduces to a point when $y = b_k$. The locus of δ_k when y describes bb_k is a two-dimensional manifold Δ_k, somewhat similar to a cone with its vertex at the point of contact of the plane $y = b_k$, and its base in the position of δ_k in H_b, and we have

$$M_2 = -\sum \lambda_k \Delta_k .$$

$$\therefore \quad (6) \qquad \Gamma \sim \sum \lambda_k \Delta_k + \text{part of } (H_b) .$$

A question may be raised as to this discussion: The difference $n' - n''$ is constant, but n', n'', may vary. Let ζ be a line separating regions in the y plane with different values of these integers, so that along ζ some of the points B_i' of one type, coincide with as many, B_i'', of the other. Is the M_2 locus of the lines A_1B_i', A_1B_i'', when y describes ζ, part of the boundary of M_3? We may deform ζ, without making it cross the critical points, so as to reduce it to a sum of the loops bb_k. This amounts to deforming the given cycle into one for which the M_2 here considered is reduced to a sum of the manifolds Δ_k, which still leads to a relation such as (6).

To return to our problem, in the particular case where $\Gamma = (C)$, the mode of derivation of the (v)'s shows at once that the coefficients λ_k in (6) are the characteristic integers of the curve C. Now from the theorem of Poincaré-Cauchy for functions of several variables it follows at once that the periods of an integral of the first kind relatively to homologous cycles are equal. But (3) extended over part of (H_b) gives zero, hence

$$\int\int_{(C)} \frac{Q(x, y, z)}{F_z'} dxdy = \sum \lambda_k \int\int_{\Delta_k} \frac{Q(x, y, z)}{F_z'} dxdy = \sum \lambda_k \int_b^{b_k} \omega_k(y)\, dy .$$

The relation (5) means then that the period of (3) relatively to the algebraic cycle (C) is zero, in accordance with Ch. I. Thus the conditions satisfied by the (λ)'s express merely that *integrals of the first kind have no periods relatively to the algebraic cycles.*

21. The converse of the property just obtained constitutes the

FUNDAMENTAL THEOREM: *A two-cycle* Γ *without periods of integrals of the first kind is algebraic.*

For if Γ satisfies (6), the corresponding period of (3) is

$$\sum \lambda_k \int_b^{b_k} \omega_k(y)\, dy ,$$

and since it vanishes there is an algebraic curve C such that to the variable part of CH_y or to this part associated with some of the points A_i correspond

the characteristic integers λ_k. Let μ_k^i be the kth characteristic integer of A_i. There is a certain two-cycle $\Gamma^i = \sum \mu_k^i \Delta_k + \text{part of } (H_b) \sim 0$ forming the boundary of the locus of $A_1 A_i$ as y describes its plane under the same conditions as above, and the (μ^i)'s are the characteristic integers of the normal functions corresponding to A_i. We may find integers t_i such that $\Gamma + \sum t_i \Gamma^i \sim \Gamma \sim \sum_k (\lambda_k + \sum_i t_i \mu_k^i) \Delta_k + \text{part of } (H_b)$, the coefficients of the (Δ)'s at the right being now the characteristic integers of the total group CH_y.

We may assume C to be variable in a continuous system with no fixed base points at the (A)'s for, if this is not so, we may replace Γ and C by $\Gamma + t(H)$ and $C + tH$, and with t sufficiently great the assumption will certainly be satisfied, especially since the (A)'s are after all arbitrary points of the surface. Let C' be a curve of the same system as C and not going through the (A)'s. C and C' have the same characteristic integers, hence

$$(C') \sim \sum_k (\lambda_k + \sum_i t_i \mu_k^i) \Delta_k + \text{part of } (H_b).$$

$(C') - \Gamma$ is then $\sim$ to a part of (H_b), and if, as it is proper to assume, H_b is irreducible, $(C') - \Gamma \sim (tH)$, which proves our theorem.

22. Given two algebraic curves C, D of V_2, if $C = D$, then also $(C) \sim (D)$. For if E is such that $C + E$ and $D + E$ are total curves of the same continuous system the cycles $(C + E)$ and $(D + E)$, reducible to each other by continuous deformation, are homologous, whence at once $(C) \sim (D)$.

I say that *conversely if* $(C) \sim (D)$, *then also* $C = D$. For we have then

$$((C - D)\ H_y) = (C\ H_y) - (D\ H_y) = [CH_y] - [DH_y] = 0,$$

and therefore C, D *have the same order.*

The axes being arbitrary, we may assume that the curves do not go through the (A)'s. Then since $(C) \sim (D)$ their characteristic integers are equal, and so are their normal functions v_h, $h \leqq p - q$. We can add to C any curve of the same continuous system as tH, and take t so great that the complete continuous systems determined by $C + tH$ and $D + tH$ contain ∞ linear systems. It may as well then be assumed that C, D already satisfy this condition. We may therefore choose a curve $C' = C$ not passing through the (A)'s and for which the (v_{p-q+k})'s are the same as for D. As C' and D have already the same normal functions of index $\leqq p - q$, these functions will all be the same for both. Since the orders are equal, C' and D are total curves of the same linear system (Poincaré), and therefore $C' = D = C$, as was to be proved.

More generally the two relations $\sum t_i (C_i) \sim 0$, $\sum t_i C_i = 0$ are equivalent. For by writing $t_i = t_i' - t_i''$, where t_i' and t_i'' are non-negative integers, they become $\sum t_i' (C_i) \sim \sum t_i'' (C_i)$, $\sum t_i' C_i = \sum t_i'' C_i$, and these relations owing to the positive sign of all coefficients are obviously equivalent.

Remark. Since $(C\ H) \not\equiv 0$, (C) is non-effective relatively to H if C is not a virtual curve. More generally, (C) is non-effective relatively to a curve belonging to a sufficiently general linear system.

23. A zero divisor Γ for two cycles is algebraic (No. 21). Since it can be considered as the difference between two algebraic cycles $(C) + \Gamma$ and (C), the corresponding algebraic curve can be considered as the difference between two curves D and C. If $\lambda\Gamma \sim 0$ for some integer $\lambda > 1$, but not for $\lambda = 1$, then also $\lambda(D - C) = 0$, this being untrue for $\lambda = 1$, so that $D - C$ is a zero divisor for the curves. Conversely if $D - C$ is a zero divisor for the curves, $(D) - (C)$ is a zero divisor for the two-cycles. If then we introduce with Severi *virtual curves*, there exists a holoedric isomorphism between the operations $+ C$ applied to the curves and $+ (C)$ applied to the cycles. We recall that, as shown by Picard and Severi, there is a maximum ρ of the number of algebraically independent curves of V_2, and that Severi has denoted by σ the order of the Abelian group formed by the zero divisors for algebraic curves, so that there are exactly $\sigma - 1$ such divisors. According to what precedes, *the number ρ is therefore equal to the number of distinct two-cycles without periods of integrals of the first kind, and σ is equal to the torsion indices σ_1, σ_2 (equal according to Poincaré).*

24. The case when the geometrical genus $p_g = 0$ leads at once to an interesting result. For then any cycle is algebraic, hence $R_2 = \rho$,

$$\rho_0 = \rho_0^2 = R_2 - \rho = 0.$$

Thus if $p_g = 0$, $\rho_0 = 0$, that is, if an *algebraic surface is without double integrals of the first kind it is also without double integrals of the second kind.* This has already been proved by Bagnera and de Franchis for irregular surfaces and for some regular surfaces,* and there is a remark by Poincaré at the end of his mémoire in the Annales de l'Ecole Normale which easily leads to the same result.

25. Assume $p_g > 0$ and consider p_g independent integrals of the first kind

$$\int\int \frac{Q_h(x, y, z)}{F_z}\, dxdy \qquad (h = 1, 2, \cdots, p_g).$$

We must have

$$\sum_{k=1}^{N} \lambda_k \int_b^{b_k} \omega_{hk}(y)\, dy = 0 \qquad (h = 1, 2, \cdots, p_g),$$

where ω_{hk} corresponds to ω_k for (3). Are these relations distinct? If they were not there would have to exist constants c_h not all zero such that

$$\sum_{h=1}^{p_g} c_h \int_b^{b_k} \omega_{hk}(y)\, dy = 0 \qquad (k = 1, 2, \cdots, N),$$

*Rendiconti del Circolo Matematico di Palermo, vol. 30 (1910), pp. 185–238.

and therefore an integral of the first kind

$$\Sigma c_h \int\int \frac{Q_h(x, y, z)}{F_z'} dxdy$$

without periods. *If we assume that this is impossible* the p_0 relations obtained are all distinct.

26. We are thus led to inquire: *Can a double integral of the first kind be without periods?* It is very likely that this question must be answered in the negative though we have succeeded in proving it only in some very special cases. For the present we merely wish to establish two relations which must exist in case the answer were affirmative.

If (3) is without periods we must have (Picard),

$$\frac{Q(x, y, z)}{F_z'} = \frac{\partial}{\partial x}\left(\frac{A(x, y, z)}{\phi(u) F_z'}\right) + \frac{\partial}{\partial y}\left(\frac{B(x, y, z)}{\phi(u) F_z'}\right),$$

where A, B are polynomials adjoint to F_2 and ϕ is a polynomial in

$$u = ax + by + cz,$$

an arbitrary linear form in x, y, z. In fact this result has been established by Picard solely for $u = y$, but the extension is at once obtained by a transformation of coördinates.

Let U, V denote the functions in parenthesis at the right and let us introduce with Picard the integral of total differentials

$$\int (-U + \epsilon) dy + V dx; \qquad \epsilon = \int^{x,z} \frac{Q(x, y, z)}{F_z'} dx.$$

It has most of the properties of those with algebraic integrands since ϵ is holomorphic everywhere except in the vicinity of the planes $y = b_k$, and there only fails to be so for certain determinations. We may reproduce almost verbatim a discussion of Severi's relating to integrals of total differentials of the second kind.* In particular we may subtract an integral $\int -Rdy + Sdx$ of total differentials with rational integrands R, S, so as to suppress the curves of infinity other than $y = b_i$ and also the periods with respect to the linear cycles of F_2. We will then have

$$\frac{Q}{F_z'} = \frac{\partial}{\partial x}(U - R) + \frac{\partial}{\partial y}(V - S) = \frac{\partial}{\partial x}\frac{A(x, y, z)}{F_z'} + \frac{\partial}{\partial y}\frac{B(x, y, z)}{F_z'},$$

where A, B are adjoint polynomials, and now the Abelian integral

$$\int \left(\frac{1}{F_z'}\right)(Ady - Bdx),$$

* Mathematische Annalen, vol. 61 (1905), pp. 20–49.

when attached to any algebraic curve C of V_2, becomes one of the first kind for that curve. Its periods with respect to an invariant cycle in a plane section are zero. It follows that it possesses all the properties of an integral of total differentials which do not require the use of the conditions of integrability in their proof. In particular we have $A = xE + A_1$, $B = yE + B_1$, where A_1, B_1, E are polynomials of order $m - 3$. However, since the invariant periods are now zero we may take E, and therefore A_1 and B_1, to be adjoint polynomials, which is certainly not the case for an integral of total differentials. Finally it may be shown that there exists an adjoint polynomial $C(x, y, z)$ such that

$$(7) \qquad AF'_x + BF'_y + CF'_z \equiv DF, \qquad A'_x + B'_y + C'_z + D \equiv Q.$$

These are the relations which we wished to derive. We observe that

$$\iint \frac{Q(x, y, z)}{F'_z}\, dxdy = \iint \frac{Q(x, y, z)}{F'_y}\, dzdx = \iint \left[\frac{\partial}{\partial x}\frac{A}{F'_y} + \frac{\partial}{\partial y}\frac{B}{F'_y}\right] dzdx,$$

and hence $C = zE + C_1$ where C_1 is adjoint of order $m - 3$.

By introducing homogeneous variables we may replace the necessary conditions for the existence of a double integral of the first kind without periods (7) by

$$(8) \qquad AF'_x + BF'_y + CF'_z + DF'_t \equiv 0, \qquad A'_x + B'_y + C'_z + D'_t \equiv Q,$$

where A, B, C, D are polynomials of order $m - 3$. We verify at once by means of a projective transformation that $\alpha A + \beta B + \gamma C + \epsilon D = 0$ cuts out on the plane $\alpha x + \beta y + \gamma z + \delta t = 0$ an adjoint of order $m - 3$ to the section of V_2 by the plane. Let us assume then that $(0, 0, 0, 1)$ is a point on the double curve. The surfaces $A = B = C = 0$ go through this point, hence it is a double point for $AF'_x + BF'_y + CF'_z = 0$, and therefore for $DF'_t = 0$, which shows that $D = 0$ also goes through the point. Hence A, B, C, D are adjoint polynomials of order $m - 3$.

27. In the whole discussion of this chapter it is possible to replace $|H|$ by any simple linear system $|E|$, ∞^2 at least, irreducible and such that when an E acquires a new singularity this consists in general in an ordinary double point. We simply take a generic pencil $\{E_u\}$ and replace everywhere y by u, the modifications being insignificant.

By considering an adequate $|E|$ on a V_2 with *arbitrary* singularities our results can be extended to it. Since $\rho_0 = R_2 - \rho$ is an absolute invariant the cycles which are gained or lost by a birational transformation are all algebraic as we already had occasion to state.

If $|E|$ is not general enough much, if not all, of the discussion is still valid. However, one may be led to neglect certain infinitesimal cycles and thus be led to the numbers $[\rho]$, $[\sigma]$ instead of ρ, σ.

In fact all this holds whenever we deal with a rational or irrational pencil such that a certain point A_1 may be uniquely determined on the generic curve of it. We can thus derive Severi's results as to the base for a surface which represents the pairs of points of two algebraic curves. The Abelian sums such as in § 1 lead at once to Hurwitz's equations for correspondences between the two curves.

28. We have studied more especially the relations between the numbers ρ, σ and certain cycles. The one to one correspondence between algebraic cycles and curves shows that to a minimum base for the cycles corresponds a minimum base for the curves and conversely. But the curves of a minimum base may well be *virtual*. It may be shown that from a base containing such curves we may always derive one composed exclusively of effective curves. There will be an effective minimum base composed of $\rho + \sigma - 1$ curves if $\rho > 1$, and of σ curves for $\rho = 1$, and in both cases an ordinary effective base composed of ρ curves (Severi).

§ 3. Extension to any V_d

29. For the sake of simplicity let us take $d = 3$. Let then $F(x, y, z, t) = 0$ be the equation of an irreducible V_3, with ordinary singularities, of order m, irregularity $\frac{1}{2}R_1 = q$ and genus of the plane sections equal to p. We designate again by $|H|$ the system of hyperplane sections, and will call $A_1, A_2, \cdots, A_m$ the fixed points of the curves $H_y H_z$. As before we shall have p integrals of the first kind attached to these curves of which $p - q$ are

$$u_h = \int \frac{P_h(x, y, z, t)}{F'_t}\, dx \qquad (h = 1, 2, \cdots, p - q),$$

where P_h is an adjoint polynomial of order $m - 3$ in x, y, t, and the q remaining integrals $u_{p-q+1}, u_{p-q+2}, \cdots, u_p$ are those of total differentials of the first kind of V_3 (Castelnuovo-Enriques).

Let C be an algebraic surface of V_3, $M_1, M_2, \cdots, M_n$ the variable points of the group $CH_y H_z$ or these points associated with some of the (A)'s. We have

$$v_h(y, z) = \sum_{s=1}^{n} \int_A^{M_s} du_h = \sum_{k=1}^{N} \frac{\lambda_k}{2\pi i} \int_{\flat}^{b_k} \frac{\Omega_{hk}(Y, z)\, dY}{Y - y},$$

$$v_{p-q+j} = \beta_j \qquad (h = 1, 2, \cdots, p - q;\ j = 1, 2, \cdots, q).$$

In these expressions the (b_k)'s are the critical values of y for the pencil $\{H_y H_z\}$ of H_z and the (β)'s are constants. Let us consider an arbitrary double integral of the first kind of H_z of the type $\int\int (1/F'_t)\, Q(x, y, z, t)\, dxdy$, where Q is an adjoint polynomial of order $m - 4$ in x, y, t. It may be easily shown that any integral of the first kind of H_z is linearly dependent upon

those of this type. We must then have

$$\sum \lambda_k \int_b^{b_k} \omega_k(y, z)\, dy = 0, \qquad \sum \lambda_k\, \omega_k(y, z) \equiv 0,$$

the (ω)'s having always the same meaning. But besides these conditions the following must also be fulfilled: When z describes a closed path the set of (λ)'s is in general returned to a different set composed of (λ')'s, the differences $\lambda_k - \lambda'_k$ forming the set of characteristic integers corresponding to the variations of the cycle (CH_z) in the manner of No. 20. As this variation is ~ 0, or, if we please, as CH_z is a uniquely determined curve on each H_z, the differences $\lambda_k - \lambda'_k$ must form a set corresponding to a system of periods, and this must be true whatever the closed path described by z.

Conversely, if all these conditions are fulfilled there exists an algebraic surface C corresponding to the functions $v_h(y, z)$. Indeed, for every z these functions determine in a unique way, that is, rationally in terms of z, a certain linear system of curves on H_z. By imposing an adequate behavior at the (A)'s we may always determine in a unique manner in this linear system, a curve the locus of which will be a surface C. More explicitly, the curve in H_y will be the intersection of the surface $F(x, y, z, t) = 0$ of the space (x, y, t) with other surfaces $\Phi(x, y, t) = 0$, where these various surfaces have no other curves in common. The (Φ)'s however may be taken to be polynomials with coefficients rational in z, whence the existence of the surface C follows immediately.

30. Let C_1, C_2, be two algebraic surfaces of V_3. If $(C_1) \sim (C_2)$, mod. V_3, $(C_1 H_z) \sim (C_2 H_z)$ mod. H_z, and therefore also mod. V_3. It follows that

$$C_1 H_z = C_2 H_z$$

in H_z and consequently C_1 and C_2 are of the same order and have the same set of characteristic integers.

We may find two surfaces D', D'', belonging to a continuous system with ∞^q linear systems and such that $C_1 + D'$ and $C_2 + D''$ belong totally to the same linear system, whence at once $C_1 = C_2$, this relation having a sense similar to that given to it for a V_2. Thus if $(C_1) \sim (C_2)$, then also $C_1 = C_2$. The converse is obviously true. We can see then that the relations

$$\sum t_i (C_i) \sim 0 \text{ mod. } V_3, \quad \sum t_i (C_i H_z) \sim 0 \text{ mod. } H_z, \quad \sum t_i C_i H_z = 0, \quad \sum t_i C_i = 0,$$

are all equivalent.* From the existence of minimum and ordinary bases

* See a different proof of the equivalence of the relations $C_1 H_z = C_2 H_z$ and $C_1 = C_2$ given by Severi in the Atti del Reale Instituto Veneto, vol. 75 (1916), p. 1138. He had already stated this proposition without proof at the end of his memoir of the Annales de l'Ecole Normale supérieure, loc. cit.—The question may be raised as to the sense to be assigned to the algebraic four-cycle (C). We know (No. 20) the sense to be assigned to the cycle (CH_z). The four-cycle in question is then to be considered as the locus of (CH_z) properly sensed associated to the z-plane sensed in a definite manner.

for the cycles follows the existence of similar bases for the curves. The variety will have numbers ρ, σ and if ρ', σ' are those of H, then $\rho \leqq \rho'$, $\sigma \leqq \sigma'$, whatever H may be.

31. The periods of the double integral attached to H_z

$$\int\int \frac{P(x, y, z, t)}{F_t'}\, dxdy, \tag{9}$$

where P is the adjoint polynomial, are of the form

$$\sum_{k=1}^{N} \lambda_k \int_b^{b_k(z)} \Omega_k(y, z)\, dy. \tag{10}$$

Let $z = c$ be a value b for which two of the upper limits, say b_1 and b_2, coincide. The author has shown (Paris Comptes Rendus, loc. cit.) that when z turns around c, (10) is increased by a multiple of the period

$$\int_b^{b_1} \Omega_1(y, z)\, dy - \int_b^{b_2} \Omega_2(y, z)\, dy; \qquad \Omega_1 = \Omega_2.$$

This will be true whether (10) is a period or not. If we develop in series of powers of Y^{-1} the differential coefficient of

$$\int\int \frac{P(x, y, z, t)}{(y - Y) F_t'}\, dxdy$$

and apply this to each term of the series we find that the period

$$\sum \lambda_k \int_b^{b_k} \frac{\Omega_k(y, z)}{y - Y}\, dy$$

increases by a multiple of

$$\int_b^{b_1} \frac{\Omega_1(y, z)}{y - Y}\, dy - \int_b^{b_2} \frac{\Omega_2(y, z)}{y - Y}\, dy.$$

In particular, for $|y|$ great enough, $v_h(y)$ $(h \leqq p - q)$ is increased by a multiple of

$$\frac{1}{2\pi i} \int_b^{b_1} \frac{\Omega_{h1}(Y, z)}{Y - y}\, dY - \frac{1}{2\pi i} \int_b^{b_2} \frac{\Omega_{h2}(Y, z)}{Y - y}\, dY.$$

I say that this and the similar expressions are not submultiples of the periods of u_h. For it vanishes for $z = c$ and if it were a submultiple of the periods the (u)'s would lose a period and $H_y H_z$ would lose a linear cycle for $z = c$, y arbitrary, which is certainly not the case if $\{H_z\}$ is generic in $|H|$.

It follows at once that the zero divisors for the curves of H_z are invariant. For otherwise a multiple of the increments of some set of (v)'s when z turns around c would form a period, hence this would be true for all sets of (v)'s in direct contradiction to what has just been found.

Thus the zero divisors for the curves of H_z are also zero divisors of V_3, whence $\sigma \leqq \sigma'$, and therefore finally $\sigma = \sigma'$, that is, *V_3 and its hyperplane sections have equal invariants σ*. As they have equal invariants σ_1, it follows that $\sigma = \sigma_1$. Here we cannot affirm any more that $\sigma = \sigma_2$. This is due to the possible existence in H_z of two-cycles not zero divisors for it but zero divisors for V_3.

32. We pass to the proof of a theorem specially important in the determination of ρ, σ, for the surfaces in V_3.

Let $c_1, c_2, \cdots, c_\nu$ be the critical values of z for $\{H_z\}$. For each of these two of the (b)'s and no more coincide. Let us make the pencil vary continuously in a net Σ containing it. The (C)'s will be displaced on an irreducible curve D if as we shall assume Σ is arbitrary in $|H|$, for when V_3 assumed in an S_4 is transformed by reciprocal polars, D is changed into a plane section of the transformed variety.

To every point c_j corresponds a well-defined two-cycle Γ_j of H_z which becomes zero for $z = c_j$ and such that when z turns around c_j any other cycle is increased by a multiple of it. I say that *if one of these cycles is algebraic so are the others*. For $\{H_z\}$ may be made to vary within Σ so as to permute c_j with c_k, thus bringing Γ_j assumed within an H_z very near H_{c_j} into Γ_k within an H_z very near H_{c_k}. Noticing that the two extreme surfaces have the same geometric genus, we infer from the theorem of No. 21 that if Γ_j is algebraic at the beginning of the deformation it will also be so at the end, that is Γ_k is then also algebraic, which proves our statement.

Suppose first that *no* Γ_k is *algebraic*. Then any algebraic cycle Δ of H_z must be invariant. For if, when z turns around c_i, Δ is returned to a cycle Δ' of H_z, $\Delta - \Delta'$ must be algebraic and as $\Delta - \Delta' \sim \mu\Gamma_k$, $\mu\Gamma_k$ must also be algebraic. Now if integrals of the first kind have no period relatively to $\mu\Gamma_k$, they have none relatively to Γ_k, and Γ_k is also algebraic. We have then a contradiction unless $\mu = 0$, $\Delta \sim \Delta'$, which shows that Δ is invariant. It follows that under our assumptions the complete systems of curves on H_z are invariant. If we take then ρ' independent continuous systems we may, as shown in No. 30, determine ρ' surfaces of V_3 whose intersections with H_z are independent curves of the surface. These ρ' surfaces will be themselves independent, hence $\rho \leqq \rho'$ and therefore since $\rho \leqq \rho'$, finally $\rho = \rho'$.

Suppose now that *the* (Γ)*'s are all algebraic*. What happens then is an immediate corollary of the following proposition, whose proof we shall do no more than outline here*: *Any two-cycle of H_z is dependent upon the (Γ)'s and the invariant cycles.*—The R_2 invariant cycles are distinct mod. V_3, hence whatever Δ, two-cycle of H_z, there is an integer λ such that $\lambda\Delta$ is homologous to an invariant cycle mod. V_3, that is $\Delta' \sim \lambda\Delta -$ invariant cycle ~ 0, mod. V_3.

* A topological proof will be found in the Borel Series monograph.

Now generalizing a discussion of Picard's (see Picard et Simart, Traité, vol. 2, p. 388), pertaining to the periods of certain integrals, and with a ready passage from periods to cycles, which shall be omitted here, it is found that the number of (Γ)'s distinct mod. H_z, (they all bound on V_3), is precisely equal to the maximum number of cycles distinct mod. H_z, but bounding on V_3. Hence Δ' depends upon the (Γ)'s, from which our assertion follows.

The application to our problem is immediate: *If the* (Γ)*'s are all algebraic, any two-cycle of* H_z *depends upon the invariant and the algebraic cycles.*

A proposition of my Annali di matematica paper taken together with a result established in a note of the Rendiconti dei Lincei of 1917 leads to this proposition: The number $\rho_0 = \rho_0^2$ of V_3 is equal to the number of non-algebraic two-cycles, or which is the same, to the number of invariant non-algebraic cycles, of H_z. We also know from Picard's work that the same number for H_z, which we shall denote by ρ_0', is equal to its total number of non-algebraic cycles. Hence if $\rho_0' > \rho_0$, H_z possesses some non-invariant non-algebraic cycles, none of the (Γ_k)'s are algebraic and $\rho = \rho'$. We may therefore state:

THEOREM. *If the number of proper integrals of the second kind of a generic hyperplane section exceeds that of* V_3, *they have equal numbers* ρ.

33. Thus for H we have $\sigma' = \sigma$, and if $\rho_0' > \rho_0$ also $\rho' = \rho$. In these conditions the trace on an arbitrary H of an ordinary base for the surfaces of V_3 forms a base for the curves of H. Let us show that if the first is a *minimum base* so is the second, this being true even if only effective surfaces or curves are considered.

Indeed let $C_1, C_2, \cdots, C_\tau$ be the surfaces of a minimum base and γ an arbitrary curve of a generic H_z. As we have seen, the complete continuous systems of curves of H_z are all invariant. Hence the complete continuous system $\{\gamma + kH \cdot H_z\}$ (k a sufficiently large integer) is invariant and contains ∞^q linear systems. One of these systems will be determined by the (β)'s, $(\beta_k = v_{p-q+k})$, and a curve γ' of it may be defined rationally on H_z by means of an adequate behavior at the points A_i, for example. The locus of γ' is an algebraic surface C going, say, l times through the curve at infinity of H_z, and we have relations such as these: $C = \Sigma \lambda_i C_i$, $H = \Sigma \mu_i C_i$, (on V_3); $CH_z = \Sigma \lambda_i C_i H_z$, $HH_z = \Sigma \mu_i C_i H_z$, (on H_z). Hence on H_z, $\gamma = CH_z - (l+k) HH_z = \Sigma [\lambda_i - (l+k)\mu_i] C_i H_z$, as was to be proved.

34. The preceding propositions remain true if we replace $|H|$ by $|E|$, ∞^3 at least, irreducible, simple, without base points, with irreducible characteristic curve E^2, such that if the surface E_0 of the system acquires singularities other than those of the generic E, they consist in general in one isolated double point, and that finally the system of the surfaces E_0 is irreducible. If $|E|$ has a base group but still irreducible variable intersection, we have the following:

Let $D_1, D_2, \cdots, D_k$ be the finite or infinitesimal curves of the base group forming base for all the surfaces of the group which are not traces of the surfaces of V_3, $D_1', D_2', \cdots, D_k'$, those forming minimum base in the same conditions. Then if $\rho_0' > \rho_0$ we have $\rho' = \rho + k$, $\sigma' = \sigma + k' - k$. Moreover, the trace of an ordinary (minimum) base of V_3 added to the (D)'s (to the (D')'s) forms an ordinary (minimum) base for E.

35. The extension to a V_d, $d > 3$, is immediate. Since V_d and its hyperplane sections have the same two-cycles the restriction $\rho_0' > \rho_0$ in the theorems just proved is now superfluous. We still have $\sigma = \sigma_1$.

The case where the two-cycles of V_d are all algebraic is especially noteworthy. H need then not be generic in its system but only without new singularities. For, let H_0 be a special H, but with the same singularities as the generic H, $C_1, C_2, \cdots, C_\gamma$ a minimum base for V_d. The two-cycles $(C_i H^{d-2})$ form a minimum base for the two-cycles of H, and as H_0 and H are homeomorphic the limiting positions $(C_i H^{d-3} H_0)$ of these cycles form a minimum base for the two-cycles of H_0.

Let now γ be any hypersurface of H_0. We have mod. H_0

$$(\gamma H^{d-3}) \sim \sum \lambda_i (C_i H^{d-3} H_0) \qquad (\lambda_i \text{ integer}).$$

But the equivalence between the relations $C = D$, $(CH^{d-2}) \sim (DH^{d-2})$, proved for $d = 2, 3$, can easily be shown to hold for any d. Applying it to H_0 we obtain $\gamma = \Sigma \lambda_i C_i H_0$, and therefore the trace of a minimum base of V_d on H_0 is a minimum base for H_0. Clearly the minimum base could everywhere be replaced by an ordinary one. It follows that H_0 has the same numbers ρ, σ as V_d.

If H_0 had special singularities of less than $d - 2$ dimensions we could only affirm that its numbers $[\rho]$, $[\sigma]$ are equal to ρ, σ respectively. Similar considerations lead to this result: Let $|E|$ be a linear system analogous to that of the same name described in No. 34 for a V_3 and without base group. If the invariant ρ_0^{d-1} of the generic E is greater than that of V_d, their invariants ρ_{d-1} are equal. Their numbers σ_{d-n}, ρ_{d-i}, $i \geqq 2$ are equal without this restriction.

36. Returning to a V_3, we may remark that there is a case where the condition $\rho_0' > \rho_0$ is certainly verified,—it is when V_3 possesses a triple integral of the first kind

$$\iiint \frac{Q(x, y, z, t)}{F_t'} dxdydz \tag{11}$$

with periods not all zero. Indeed its periods relatively to cycles within H_z are all zero, as follows from the discussion at the end of the first chapter. Hence there must be periods relatively to finite cycles or special cycles such

as described in proposition (b) of No. 2. This in turn requires that the double integral of the first kind attached to H_z,

$$\iint \frac{Q(x, y, z, t)}{F'_t}\, dxdy \tag{12}$$

be not without periods. But the periods of (12) relatively to algebraic cycles are zero, and those relatively to invariant cycles are rational in z, finite everywhere, infinitesimal for z infinite, and therefore also zero. Hence the cycles Γ_k of No. 32 are not algebraic and $\rho' = \rho$ for $|H|$ or for any linear system without base group such as $|E|$, already described. This may also be shown by remarking that (12) is not improper of the second kind and since it is without invariant periods it cannot be derived from an integral of the second kind of V_3, consequently $\rho'_0 > \rho_0$.

Let us now take a V_d and call Γ a d-cycle relatively to which one of its d-uple integrals of the first kind has a non-zero period. Γ may be the sum of two cycles, the first Γ' being contained in H and the second Γ'' of the special type described in proposition (b), No. 2. If the period relatively to Γ'' is not zero the reasoning just used for V_3 applies here and we shall find that H possesses a $(d-1)$-uple integral of the first kind with at least one non-zero period. On the other hand if the period relatively to Γ' is not zero we may by reasoning as in No. 15, Chapter 1, show that there is a $(d-2)$-uple integral of the first kind of H^2 having at least one non-zero period. Continuing this we shall come either to an H^{d-3} or to an H^{d-2} with integrals of the first kind of multiplicity $d-3$ or $d-2$ having at least one non-zero period. In the first case it follows at once that H^{d-2} has the same number ρ as H^{d-3} and therefore as V_d, its bases being the traces of those of V_d. In the second case the reasoning applied for V_3 holds as between H^{d-3} and H^{d-2}, leading to the identical conclusion.

As an application, a generic V_2, complete intersection of $d-2$ hypersurfaces in a V_d, each generic in an adequate linear system, has for bases the traces of those of V_d, provided there is a d-uple integral of the first kind of V_d with periods not all zero.

The most interesting case is that of an Abelian variety of *genus* p and rank *one*, for if $u_1, u_2, \cdots, u_p$ are the variables occurring in its parametric representation $\int\int\cdots\int du_1\, du_2 \cdots du_p$ is an integral of the first kind with at least one non-zero period.

37. For a V_d, $d > 2$, contrary to what happens for an algebraic surface, the number of two-cycles without periods for the integrals of the first kind is only a maximum of ρ. At all events we have succeeded in proving that these two numbers are equal only for Abelian varieties, as we shall see in the second part, and for a certain type of V_3, which may be defined thus: let P_a, P_g be

respectively the arithmetic and geometric genus of a V_3. *If* $P_g - P_a + q = 0$, *all the two-cycles are algebraic, and therefore* ρ *reaches its maximum.* Indeed as shown by Severi, in this case the system adjoint to $|H|$ cuts out the complete canonical system on H. Hence every double integral of the first kind of H_z is a linear combination of those of type $\int\int (1/F_t)Q(x, y, z, t)\,dxdy$, where Q is adjoint of order $m - 4$, whose periods relatively to invariant cycles all vanish. It follows then that all these cycles are algebraic cycles of H_z and, being invariant, they are also algebraic cycles of V_3. In this case $\rho_0 = R_2 - \rho = 0$, hence $\rho = R_2$.

§ 4. Some applications

38. *Complete intersections.* Let V_2 be a non-singular algebraic surface, complete intersection of $(r-2)$ varieties in an S_r. I say that V_2 has no double integrals of the first kind without periods. For let $F(x, y, z) = 0$ be the equation of its projection V_2' in an S_3. It is sufficient to show that there can be no relation $AF_x' + BF_y' + CF_z' \equiv -DF$, where A, B, C are adjoint of order $m-2$. For according to this relation the N contacts of the planes $y = Ct$, tangent to V_2', must be on $B = 0$. Now if $|K|$ designates the canonical system and $|H|$ the complete system of the plane sections, the adjoint surfaces of order $m-2$ cut out on V_2' the system $|K + 2H|$. They intersect the first polar of an arbitrary point of S_3 in a number of points exterior to the double curve, at most equal to*

$$[(K + 2H)(K + 3H)] = [K^2] + 5[KH] + 6[H^2],$$

and hence it is only necessary to prove that this number is $< N$. Let $m_1, m_2, \cdots, m_{r-2}$, be the orders of the varieties of S_r of which V_2 is the intersection. Then $m = m_1 m_2 \cdots m_{r-2}$, and the adjoint system is cut out on V_2 by the varieties of order $n = \Sigma m_i - r - 1$; therefore $[K^2] = mn^2$, $[KH] = mn$, $[H^2] = m$. Hence the number considered above is equal to $mn^2 + 5mn + 6m$. To find the value of N we observe that in S_r the hyperplanes of a linear net which are tangent to V_2 touch the surface at the points where it is intersected by a variety of order $n+3$, hence $N = m(n+3)^2 > mn^2 + 5mn + 6m$, which proves our assertion.

This still applies when all the (m)'s are equal to unity except for one which is > 3, that is, when we deal with a non-singular algebraic surface of order > 3 in ordinary space.

39. Now a non-singular V_{r-1} in S_r, $r > 3$, has for minimum base the trace of a minimum base of S_r, that is, a hyperplane section. Its index $R_2 = 1$ as it is for S_r and its two-cycles are all algebraic. Its complete systems of hyper-

* It is in general less than this number by a certain multiple of the number of pinch points owing to the peculiar behavior of the first polars at these points.

surfaces are all linear. Here then, equivalence à la Severi between two hypersurfaces implies that they are contained in the same linear system, and as they are all multiples of a hyperplane section, V_{r-1} *contains only hypersurfaces which are complete intersections.* The same reasoning holds for its intersection with another non-singular V_{r-1} of S_r, provided that this intersection is non-singular and also that $r > 4$, and so on. We thus see that *a non-singular* V_d, $d > 2$, *complete intersection in an* S_r, *contains only hypersurfaces that are themselves complete intersections.*

Let now $d = 2$. Any V_3, complete intersection and non-singular, passing through V_2, possesses no proper double integrals of the second kind since its $R_2 = \rho$, whereas V_2 certainly possesses such an integral if its order is > 1 and no space of less than four dimensions can be passed through it, or, as this is usually stated, if it is *normal* in an S_r, $r > 3$. Hence *a non-singular* V_2, *complete intersection and normal in an* S_r, $r > 3$, *contains in general only curves which are complete intersections.* This is true also for a non-singular surface of order > 3 in ordinary space.* For ordinary space this theorem has been stated and proved many years ago by Noether, but his proof based on enumeration of constants has long been considered unsatisfactory. The above is believed to be the first complete proof ever given of this important proposition.

As shown previously, even limiting ourselves to ordinary space, we can go farther. Let $|E|$ be a linear system, simple, irreducible, ∞^3 at least, with a base group composed of k curves independent on E and such that no point is multiple for any E through it. The generic E contains no other curves than those cut out by surfaces passing through curves of the base group, and for it $\rho = k + 1$, $\sigma = 1$.

40. The part of our results relating to a V_{r-1} in S_r, $r > 3$, has already been obtained by Severi. The cubic variety in S_4, (Segre variety), has been treated at length by G. Fano. It furnishes a very interesting illustration. Indeed it may be verified that when there are less than six double points the variety belongs to a linear system, ∞^4 at least, and with the properties described more than once, hence it contains only complete intersections. For the hyperplane sections whose geometric genus is zero, $\rho = 7$. Intersections with hypersurfaces of order $\leqq 2$ contain in general only complete intersections.

41. *Double plane.* Let $z^2 = f(x, y)$ be the equation of a double plane. One may always transform it birationally so that the branch curve be of even order $2m$, without multiple components and with multiple points all of even order and with distinct tangents. Any double integral of the first kind is of

* During the final preparation of this memoir the author's attention was attracted by an incomplete proof of these theorems due to G. Fano, (Torino Atti, vol. 44 (1909), pp. 415–430) which has some points in common with the one given here. Fano admits that a double integral of the first kind cannot be without periods, and this can scarcely be considered as axiomatic.

the form $\int\int [f(x,y)]^{-\frac{1}{2}} Q(x,y,t)\,dxdy$, where Q is a polynomial of order $m-3$ and has an $(i-1)$-uple point at a $2i$-uple point of $f(x,y)$, (Enriques). If the periods are zero one may show that equations (8) now become $A'_x + B'_y + C'_t \equiv Q(x,y,t)$, $Af'_x + Bf'_y + Cf'_t \equiv 0$, where A, B, C are of order $m-1$ and behave like Q at the multiple points of f. Here again the points of intersection, other than the multiple points of $f=0$, of the curves $f'_x = 0, f'_y = 0$, must be on $C=0$. Hence $C=0$ and $f'_x = 0$ have in common at least

$$(2m-1)^2 - \sum (2i-1)^2 + \sum (2i-1)(i-1) = (2m-1) - \sum i(2i-1)$$

points, the summation being extended to all the multiple points. To show that our double integral cannot be deprived of periods it is sufficient to show that this number exceeds $(m-1)(2m-1)$, which, since $f'_x = 0$ may be assumed irreducible, will lead to an impossibility. But the inequality to be proved reduces at once to $m(2m-1) > \Sigma\, i(2i-1)$ which is actually verified, for it may be obtained by expressing that the number of isolated double points equivalent to the multiple points of $f(x,y)$ does not exceed its value $m(2m-1)$ when f is a product of $2m$ linear factors. Thus *a double plane has no double integral of the first kind without periods.*

42. When does a double plane belong to a linear system with the properties described in No. 34? I say that this will certainly occur if $f(x,y)$ is divisible by a factor $\phi(x,y)$ such that the curve $\phi(x,y)=0$ be generic in a linear system $|\gamma|$, ∞^2 at least, not composed with the curves of a pencil, and such that there is no point not a base point multiple for any γ through it. For let $f \equiv \phi\cdot\psi$, and $\phi + k\phi_1 = 0$ the equation of a generic pencil of $|\gamma|$. First we verify that the variable curve of intersection of the two surfaces $z^2 = \phi\psi$, $z^2 = (\phi + k\phi_1)\psi$, is irreducible. Indeed if it were not the two surfaces would have the same tangent planes at the points $z = \phi = \phi_1 = 0$ which are not base points for $|\gamma|$, and the curves $\phi = \phi_1 = 0$ would be tangent at those points, which is not the case. Next the multiple points of the double plane are the multiple points of $f=0$, and a fixed $(2m-2)$-uple base point at infinity, hence there is no point other than a base point multiple for all the double planes having for branch curve $\psi = 0$ associated with a curve γ, and we can apply our general theorems to them.

43. To find the minimum base we must first determine whether the components of the branch curve are independent curves of the double plane. Let $f \equiv \phi_1\cdot\phi_2\cdots\phi_h$, where the (ϕ)'s are irreducible polynomials prime to each other, and let C_i be the curve $\phi_i = 0$ of the double plane. Denoting by $|H|$, $\{H_y\}$ the same elements as usual, we consider $m-1$ independent integrals of the first kind $u_1, u_2, \cdots, u_{m-1}$ of H_y and observe that since in

the case here considered the double plane is *regular* (Castelnuovo-Enriques), a relation $\Sigma t_i C_i = 0$ would necessarily lead to another

$$\sum_{i,j} t_i \int_{(x,\bullet)}^{M_{ij}} du_s = 0 \qquad (s = 1, 2, \cdots, m-1),$$

where the points M_{ij} are the points of the group $C_i H_y$, and the lower limit of integration is arbitrary on H_y. Now H_y is hyperelliptic of genus $m-1$, and, as far as the integrals at the left are concerned, one may be made zero, while their sum vanishes. We also know that by combining them linearly with suitable integral coefficients we obtain $2m-2$ independent periods of u_s. Hence the only relation of the type considered corresponds to

$$t_1 = t_2 = \cdots = t_h = t,$$

and as we have $t \Sigma C_i = tH \not\equiv 0$, the (C)'s are actually independent.

We conclude from this that if $p_g > 0$ and one of the (C)'s is variable in a suitable linear system, the minimum base is composed of: (*a*) The vicinity of the singular point at infinity on the z axis which counts for h curves. (*b*) The vicinities of the multiple points of the branch curve which will count for, say, k curves. The value of k will depend upon the nature of the singular points, etc. In the simplest case where the curve has only ordinary double points k will be equal to their number.

(*c*) The h components of the branch curve. We have therefore $\rho = 2h + k$, $\sigma = 1$, $[\rho] = h$. Every curve of the double plane is cut out by a surface which goes through several of the (C)'s and through no other curve of the double plane.

As to ρ_0, it may be computed thus: If N is the class of the branch curve, d the equivalence in double points of its multiple points we find by means of $\{H_y\}$, $[R_2'] = N - 6m + 5 + d$. Therefore

$$\rho_0 = [R_2'] - [\rho] + 1 = N - 6m + 6 + d - h.$$

This discussion can be applied to derive some of Picard's results for double planes as well as some due to Enriques for surfaces of linear genus $p_1 = 1$. Let us take for example the surface $z^2 = a(y)x^3 + b(y)x^2 + c(y)x + d(y)$, where a, b, c, d, are polynomials, a surface considered by Picard.* If these polynomials are arbitrary and prime to each other the double plane contains only complete intersections and this relation cannot be satisfied by substituting for z and x rational functions of y.

Enriques showed that the surfaces named after him are reducible to double planes, the determination of their minimum base as he gave it is then immediate.† These double planes contain also only complete intersections.

* Picard-Simart, *Traité des fonctions algébriques de deux variables*, vol. 2, p. 268.

† Rendiconti dei Lincei, ser. 2, vol. 23 (1914), pp. 291–297.

§ 5. Varieties representing the groups of points of other varieties

44. We insert here a short discussion of these varieties that will be found useful in some applications. They present also the added interest that we can form very readily varieties of this type having quite arbitrary torsion indices.

Let then $V^1, V^2, \cdots, V^n$ be algebraic varieties with ordinary singularities, d_i the dimensionality of V^i, V_d a variety representing without exception the groups of n points of which each is on a V^i, so that $d = \Sigma\, d_i$.

By generalizing somewhat the reasoning at the beginning of this paper, it may be shown that all the i-cycles are sums of those obtained by associating an i_1-cycle of V^1, an i_2-cycle of V^2, $\cdots$ $(i_1 + i_2 + \cdots = i)$ in the same manner as $V^1, V^2, \cdots$. Let then R_i^h, R_i and σ_i^h, σ_i be the ith indices of connectivity and torsion of V^h and V_d respectively. We shall have $R_i = \Sigma\, R_{i_1}^1 R_{i_2}^2 \cdots R_{i_n}^n$, the summation being extended to all the partitions of the (i)'s such that $i = i_1 + i_2 + \cdots + i_n$, $i_h \leqq 2d_h$, and with the convention that $R_{2d_h}^h = R_0^h = 1$.

As to the (σ)'s suffice to state that $\sigma_1 = \sigma_1^1\, \sigma_1^2 \cdots \sigma_1^h$. Now Godeaux has shown that there are algebraic surfaces whose invariant $\sigma = \sigma_1$ is any odd prime, and an example of $\sigma = 2$ has been given by Severi. This shows that there are algebraic varieties for which σ has any value whatever. We shall have occasion to consider in the second part Abelian varieties of rank > 1 whose invariant σ is arbitrarily assigned and in fact equal to the rank. Suitable surfaces contained in these varieties will have the same value of σ, i.e., equal to an arbitrary integer.

Remark. All the varieties so far known, including those to be constructed in the second part, for which $\sigma > 1$, represent involutions on varieties whose $\sigma = 1$. The question presents itself—are there any others? For the present it must remain unanswered.

45. Let us now pass to the determination of ρ. Assume first $n = 2$. V_d contains a continuous system ∞^{d_1}, Σ_1, of varieties identical with V^2 and another ∞^{d_2}, Σ_2, of varieties identical with V^1. A hypersurface of V_d representing the pairs of points of V^2 and a hypersurface of V^1 will be called *fundamental* for V^1. Similarly there will be hypersurfaces fundamental for V^2. The hypersurfaces fundamental for V_i possess an ordinary (minimum) base composed of ρ_i, $(\rho_i + \sigma_i - 1)$, hypersurfaces. Assume that E_i is fundamental for V^i. Then certainly there can be no relation $E_1 = E_2$ since the homology $(E_1) \sim (E_2)$ is not verified. Hence the hypersurfaces of the two fundamental sets are not related.

To find the number of hypersurfaces independent of those of the fundamental sets, I say that if $d_1 \geqq 3$, V^1 may be replaced by a V_{d_1-1} having the

same Picard variety W_1 as V^1. For let $\{C_\mu\}$ be an arbitrary linear pencil of hypersurfaces fundamental for V_1. If A, B are two hypersurfaces such that $AC_\mu = BC_\mu$ on any C_μ, then $A - B$ is fundamental for V^1. This can be shown in a manner very similar to that used to prove the analogous theorem for any V_3 and the pencil $\{H_z\}$. If $\{C_\mu\}$ were generic in a suitable linear system we would have $A = B$, but here we may only conclude that $A - B$ is a multiple of C_μ. It follows then that as far as we are concerned V^1 may be replaced by C_μ whose Picard variety will be W_1, if $d_1 \geqq 3$.

We propose to show next that just as in the case $d_1 = d_2 = 1$ already investigated by Severi,* the number of hypersurfaces independent of those of the two fundamental sets is equal to Scorza's simultaneous index λ_{12} of the Picard varieties W_1, W_2 of V_1 and V_2. This index will be defined in the second part (No. 47). We may then assume $d_1 \leqq 2$, $d_2 \leqq 2$, $d_1 + d_2 > 2$. One of the (d)'s, say d_1, will have the value *two*.

Let A be an arbitrary hypersurface of V_d, $\{C_1\}$ a complete continuous system of curves of V^1 containing ∞^{q_1} linear systems, (q_i irregularity of V^i), C_1^1 the fundamental hypersurface determined by C_1. To the points $C_1^1 A$ may correspond either all the points of V^2 or only a V_{d_2-1} of V^2. The first case may be rejected at once for then there corresponds to the points in question only a finite number of points on C_1, and to A only a curve on V^1; hence A is fundamental. In the second case, to which we may limit ourselves then, there corresponds to $C_1^1 A$ a certain algebraic curve C_2 on V^2 if $d_2 = 2$, or a group of points if $d_2 = 1$. But C_1 determines a point of W_1 and C_2 one of W_2, for by adding if necessary a suitably chosen fundamental hypersurface to A, we may arrange matters so that C_2 belongs to a continuous system containing ∞^{q_2} linear systems. We have here an algebraic correspondence between the points of W_1 and W_2 and the theory of Hurwitz-Severi may be extended at once, leading to the announced result. The extension to $n > 2$ is immediate. It is sufficient to consider V_d as corresponding to the group of two points one of which is on V^1 and the other on the V_{d-d_1}, obtained by associating $V^2, \cdots, V^n$. We shall have finally $\rho = \Sigma\, \rho^{(i)} + \Sigma\, \lambda_{ik}$, where $\rho^{(i)}$ is the number ρ of V^i and λ_{ik} the simultaneous index of the Picard varieties of V^i and V^k.

* Torino Memorie, ser. 2, vol. 54 (1903), pp. 1–49.

PART II

ABELIAN VARIETIES

CHAPTER I. GENERAL PROPERTIES

§ 1. A summary of certain fundamental theorems and definitions

46. An *Abelian* variety of genus p, V_p, is a variety whose non-homogeneous point coördinates are equal to $2p$-ply periodic meromorphic functions of p arguments $u_1, u_2, \cdots, u_p$, or whose homogeneous point coördinates are proportional to theta's of the same order and continuous characteristic. The variety is algebraic (Weierstrass) and of dimensionality p. When the periods are those of a set of independent integrals of the first kind of a curve of genus p, V_p is called a *Jacobi* variety.

An array with p rows and $2p$ columns

$$\Omega \equiv \| \omega_{j\mu} \| \quad (j = 1, 2, \cdots, p;\ \mu = 1, 2, \cdots, 2p)$$

is the period matrix of a V_p provided that:

(a) There exists an alternate bilinear form with rational coefficients

$$\sum_{\mu,\nu=1}^{2p} c_{\mu\nu} x_\mu y_\nu, \qquad c_{\mu\nu} = -c_{\nu\mu}, \tag{1}$$

vanishing identically when the (x)'s and the (y)'s are replaced by the elements of any two rows of Ω.

(b) If we set $\xi_\mu + i\eta_\mu = \Sigma_{(j)} \lambda_j \omega_{j\mu}$, then, for all non-zero values of the (λ)'s, $\Sigma c_{\mu\nu} \xi_\mu \eta_\nu > 0$. According to Scorza ($b$) is equivalent to this: Denoting by $\bar{x}$ the conjugate of any number x, the Hermitian form in the (λ)'s,

$$\sum A_{jk} \lambda_j \lambda_k, \qquad A_{jk} = -\frac{1}{2i} \sum c_{\mu\nu} \omega_{j\mu} \bar{\omega}_{k\nu}, \tag{2}$$

must be definite positive. When these conditions are satisfied Ω is called by the same author a *Riemann matrix*.

47. We propose now to recall some concepts and definitions incipient in the works of various authors, but formally introduced and only fully developed in recent writings of Scorza and also Rosati.* The nomenclature which we shall use is Scorza's.

The alternate form (1) is called a *Riemann form* of Ω. If the condition (b) is satisfied for that form, it is said to be a *principal* form of the matrix. There

* See Scorza's memoir in the Rendiconti di Palermo, vol. 41 (1916), for numerous bibliographical indications. The very interesting method which dominates his and Rosati's investigations had been used previously without their being apparently aware of it by Cotty in his Paris thesis (1912) for the case $p = 2$. Cotty attributes the idea to Humbert. We shall have opportunity to apply it on several occasions.

may be several independent forms alternate of Ω, and if $1 + k$ is their number, k is called the *index of singularity*. If $k \neq 0$ the matrix is said to be *singular*.

There may be $1 + h$ bilinear forms with rational coefficients

$$\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\, x_\mu\, y_\nu \tag{3}$$

vanishing identically when the (x)'s and the (y)'s are replaced by the elements of any two rows of Ω. The integer h is called the *index of multiplication*, and we have $h \geqq k$.

Finally, given two Riemann matrices Ω, Ω', if there exist λ bilinear forms with rational coefficients

$$\sum c_{\mu\nu}\, x_\mu\, y_\nu \quad (\mu = 1, 2, \cdots, 2p;\ \nu = 1, 2, \cdots, 2p';\ p, p' \text{ genera of } \Omega, \Omega') \tag{4}$$

which vanish identically when the (x)'s are replaced by the elements of a row of Ω and the (y)'s by those of a row of Ω', λ is called the *index of simultaneity* of the two matrices.

The forms of types (1), (3), (4), generate moduli and admit bases. The corresponding numbers σ are all equal to *one*.

Two matrices Ω, Ω' are *isomorphic* if we can pass from one to the other by a linear transformation with arbitrary coefficients applied to the rows and by a linear transformation with rational coefficients applied to the columns. If this last transformation is of determinant one and integral coefficients (unimodular), Ω, Ω' are *equivalent*. In all cases the determinants of the two transformations must not be zero. When two matrices are isomorphic, the most general Abelian varieties which correspond to them in the sense defined below, are in algebraic correspondence with each other. When the matrices are equivalent, their Abelian varieties can be transformed birationally into each other.

A Riemann matrix Ω is said to be *impure* if it is isomorphic to one of type

$$\left\| \begin{matrix} \Omega_1, & 0 \\ 0, & \Omega_2 \end{matrix} \right\|,$$

where Ω_1, Ω_2, are Riemann matrices of genus p and the ciphers represent matrices with elements all zero. If Ω is not impure, it is said to be *pure*. When Ω is impure the field of Abelian functions which belongs to it contains functions of genus $< p$, (Poincaré). Finally, in the same case, an Abelian variety belonging to Ω represents the pairs of points, one of which is on an Abelian variety belonging to Ω_1 and the other on one belonging to Ω_2.

The results at the end of the preceding part allow us to replace the determination of the base invariants of an impure variety by that of the invariants of varieties of genus $< p$. We shall return to this point later.

Remark. All the properties which we have recalled here are invariant in regard to isomorphism.

48. The matrix Ω is equivalent to a matrix in the so-called *canonical* form

$$A \equiv \begin{Vmatrix} \frac{1}{e_1}, & 0, & \cdots & 0 & a_{11}, & a_{12}, & \cdots & a_{1p} \\ 0, & \frac{1}{e_2}, & \cdots & 0 & a_{21}, & a_{22}, & \cdots & a_{2p} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & \cdot & \cdots & \frac{1}{e_p} & a_{p1}, & \cdot & \cdots & a_{pp} \end{Vmatrix} \quad (a_{jk} = a_{kj}),$$

where the integers e_μ are the elementary divisors of (1), assumed now with integral coefficients. The matrix has a principal form $\Sigma_{\mu=1}^{p} e_\mu (x_\mu y_{p+\mu} - x_{p+\mu} y_\mu)$ derived from (1) up to an integral factor, and condition (*b*) gives now this: If $a_{jk} = a'_{jk} + ia''_{jk}$, the quadratic form $\Sigma\, a''_{jk} x_j x_k$ must be definite positive, or, which is the same, $\Sigma\, a''_{jk} x_j x_k = 1$ must be a real generalized ellipsoid. The arbitrariness of the (a'')'s shows that in general the above alternate form is unique—that is, that for an arbitrary Riemann matrix $k = 0$.

Let us indicate a certain property of the Hermitian form (2), interesting especially in some applications. Designate by C an arbitrary alternate Riemann form of Ω, for example (1), then apply a transformation B of non-zero determinant defined by

$$\omega'_{j\mu} = \sum_{\nu=1}^{2p} b_{\mu\nu}\, \omega_{j\nu}$$
$$(\mu = 1, 2, \cdots, 2p;\ j = 1, 2, \cdots, p).$$

To the matrix of the (ω')'s will correspond an alternate form C' defined in the notation of Frobenius by $C' = \overline{B}^{-1} C B^{-1}$, where $\overline{B}$ is the transposed of B.

Consider now the transformation D defined by the matrix

$$\begin{Vmatrix} \omega_{11}, & \omega_{12}, & \cdots & \omega_{1,2p} \\ \cdot & \cdot & \cdot & \cdot \\ \omega_{p1}, & \cdot & \cdots & \omega_{p,2p} \\ \overline{\omega}_{11}, & \cdot & \cdots & \overline{\omega}_{1,2p} \\ \cdot & \cdot & \cdot & \cdot \\ \overline{\omega}_{p1}, & \cdot & \cdots & \overline{\omega}_{p,2p} \end{Vmatrix}$$

whose determinant as we know is not zero. Applying finally to the (ω)'s the transformation $\overline{D}^{-1}$, the form C will be replaced by a form C'' of same genus $q \leqq p$ as C, that is, depending essentially upon the same number of linearly distinct variables, ($2q$ for the (x)'s, $2q$ for the (y)'s), as C. But owing to the relations $\Sigma\, c_{\mu\nu}\, \omega_{j\mu}\, \omega_{k\nu} = \Sigma\, c_{\mu\nu}\, \overline{\omega}_{j\mu}\, \overline{\omega}_{k\nu} = 0$, we find that the matrix of the coefficients of C'' is equal to the product of 2^{2p} by

$$\begin{Vmatrix} 0, & A \\ \overline{A}, & 0 \end{Vmatrix},$$

where A is the matrix $||A_{jk}||(j, k = 1, 2, \cdots, p)$. If we call genus of a Hermitian form the number of essentially distinct variables upon which it depends, we see *that the genus of an alternate Riemann form of* Ω *is equal to that of the corresponding Hermitian form.*

50. *Rank of Abelian Varieties.* Let us transform Ω into a canonical matrix and, using the same notations as in Krazer's *Lehrbuch der Thetafunctionen*, consider the equations

$$\tau x_j = \theta_k^j \begin{bmatrix} g \\ h \end{bmatrix}(u) \qquad (j = 1, 2, \cdots, s > p), \tag{5}$$

where the (θ)'s are linearly independent theta-functions of sufficiently high order k belonging to A. The (x)'s are point coördinates of an Abelian variety belonging to A, or if we wish to Ω. Let $v_1, v_2, \cdots, v_p$ be the variables corresponding to Ω. To every system of values of the (v)'s corresponds one and only one of the (u)'s modulo the periods of A, and conversely to every system of values of the (u)'s corresponds one and only one of the (v)'s modulo the periods of Ω. The relations $v_h = \Sigma_{\mu=1}^{2p} t_\mu \omega_{h\mu} (h = 1, 2, \cdots, p)$, where the (t)'s are real variables such that $0 \leqq t_\mu < 1$, define for each system of values of the (u)'s, or the (v)'s, a unique point of an S_{2p} of which the (t)'s are considered as non-homogeneous point coördinates. The point-set thus obtained fills up a generalized cube U_{2p}, at least if we assume, as we may, that the axes of the (t)'s in S_{2p} are rectangular. We shall make frequent use of this generalized cube. We could have defined it in terms of the (u)'s but for certain applications it is more advantageous to relate directly Ω, and U_{2p}.

Now, to every point of U_{2p} corresponds one and only one of V_p. However, it may be that to any point of V_p there correspond more than one of U_{2p}. Let r be the number of these points. It has been called by Enriques and Severi the *rank* of V_p.

Let us show that *the most general Abelian variety belonging to* V_p *is of rank one.* If V_p is such a variety it will be possible to express every periodic function belonging to Ω as a rational function of the (θ_k)'s. Assume this condition fulfilled and let (u), (u') be two points of U_{2p} which correspond to the same point of V_p. We shall have

$$\frac{\theta_k^1(u)}{\theta_k^1(u')} = \frac{\theta_k^2(u)}{\theta_k^2(u')} = \cdots = \frac{\theta_k^s(u)}{\theta_k^s(u')}.$$

But the periodic functions are in fact rational in the ratios of (θ_k)'s, hence they take the same values at (u) and (u'). This will be the case in particular for the ratios of the functions $\theta_k(u - e)$, since they are periodic. It follows that the above system will still be satisfied when the (u)'s and the (u')'s are replaced by the quantities $u_i - e_i$, $u'_i - e_i$ respectively, the (e)'s being any

constants. Hence, if we replace u_i by $u_i + du_i$ we must, in virtue of the functional relationship thus established, replace u'_i by $u'_i + du_i$. Otherwise stated

$$du'_i = \frac{\partial u'_i}{\partial u_1} du_1 + \frac{\partial u'_i}{\partial u_2} du_2 + \cdots + \frac{\partial u'_i}{\partial u_p} du_p = du_i$$

$$\therefore \frac{\partial u'_i}{\partial u_k} = 0, \quad i \neq k; \qquad \frac{\partial u'_i}{\partial u_i} = 1; \qquad u'_i = u_i + \omega_i.$$

The (ω)'s form a system of constants which may be added to the (u)'s without changing the values of the ratios $\theta'_k[{}^{r}_{k}](u)/\{\theta'_k[{}^{r}_{k}](u)\}$. They are therefore simultaneous periods of these periodic functions, and the points (u), (u') coincide, which means that $r = 1$.

Thus to every Riemann matrix, corresponds a class of Abelian varieties of rank one and they are obviously birationally equivalent.

51. Let us show that *amongst the varieties of rank one, there exists always one without singularities situated in a suitable space and in point to point correspondence without exception with* U_{2p}.

Let us start again from the representation (5) where we shall assume the (θ_k)'s such that any other θ of the same order and characteristic is a linear combination of them. Two circumstances may prevent that V_p as represented by equations (5) satisfy the desired conditions.

(*a*) All the (θ_k)'s vanish for at least one point, (u).

(*b*) There exists at least one point, (u), for which the hyperplanes of $S_{\rho-1}$ represented by

$$\begin{Vmatrix} x_1 & x_2 & \cdots & x_\rho \\ \theta_k^1 & \theta_k^2 & \cdots & \theta_k^\rho \\ \dfrac{\partial \theta_k^1}{\partial u_1} & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \dfrac{\partial \theta_k^1}{\partial u_p} & \cdot & \cdots & \cdot \end{Vmatrix} = 0$$

have in common a space of more than p dimensions or, if we prefer, there exists at least one point, (u), for which the array

$$\begin{Vmatrix} \theta_k^1 & \theta_k^2 & \cdots & \theta_k^\rho \\ \dfrac{\partial \theta_k^1}{\partial u_1} & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \dfrac{\partial \theta_k^1}{\partial u_p} & \cdot & \cdots & \cdot \end{Vmatrix}$$

is of rank $< p + 1$.

Let W be the manifold of U_{2p}, or, if we please, the algebraic sub-variety

of V_p for which either circumstance presents itself. The question is to show that for a suitable choice of the representation (5) there is no manifold of this nature. Let us remark first that among the functions $\theta_{nk}\left[\begin{smallmatrix} g \\ h \end{smallmatrix}\right]$ are found the $\left(\theta_k\left[\begin{smallmatrix} (g+a)/n \\ (h+b)/n \end{smallmatrix}\right]\right)^n$ (a, b, integers). Hence if, whatever the representation (5), W contained points of type (a), the functions $\theta_k\left[\begin{smallmatrix} (g+a)/n \\ (h+b)/n \end{smallmatrix}\right](u)$, would all have a point in common. Since for n great enough there is a characteristic $\left[\begin{smallmatrix} (g+a)/n \\ (h+b)/n \end{smallmatrix}\right]$ differing as little as we please from any given one, by passing to the limit, we could conclude that the (θ)'s of a given order all vanish at a point (u_0) of V_p. This is equivalent to stating that for any θ_k,

$$\theta_k(u_1^0 - e_1, u_2^0 - e_2, \cdots, u_p^0 - e_p) = 0,$$

whatever the (e)'s, or else $\theta_k \equiv 0$.

Thus, when the characteristic is arbitrary, case (a) will certainly not present itself.

Let us show now that case (b) may as well be avoided. Consider the representation

$$\tau x_i = \theta_{nk}^i\left[\begin{smallmatrix} g \\ h \end{smallmatrix}\right](u) \qquad (j = 1, 2, \cdots, s'),$$

where s' is the dimension of the linear system of (θ)'s of order nk and given characteristic and let W' be the singular subvariety corresponding to it. For k great enough, the functions $\theta_k\left[\begin{smallmatrix} g/n \\ h/n \end{smallmatrix}\right](u)$ will not all vanish at the same point. But the functions $\left(\theta_k^i\left[\begin{smallmatrix} (g+a)/n \\ (h+b)/n \end{smallmatrix}\right](u)\right)^n$ are linear combinations of the (θ_{nk}^i)'s of our representation. Let s be the dimension of the system of the (θ_k)'s of given characteristic. We can choose s functions $\theta_k\left[\begin{smallmatrix} (g+a)/n \\ (h+b)/n \end{smallmatrix}\right](u)$ not vanishing at a given point A of W'. Let us form the matrix which defines W' by taking for functions relatively to its s first columns, the nth powers of these s functions. One can then verify at once that A must belong to the W which corresponds to the representation by the $\theta_k\left[\begin{smallmatrix} (g+a)/n \\ (h+b)/n \end{smallmatrix}\right](u)$. But these subvarieties W are all the transformed of one and the same one by ordinary transformations of the first kind, transformations in as great a number as desired provided n is great enough.* When n exceeds a certain limit, they certainly do not have any common points, hence for the representation then obtained by means of the functions $\theta_{nk}\left[\begin{smallmatrix} g \\ h \end{smallmatrix}\right](u)$ with arbitrary characteristic, neither case (a) nor case (b) will present itself, and the theorem is proved.

The importance of this theorem is due to the fact that a number of propositions on varieties of more than two dimensions are not applicable when the singularities are not ordinary. We may mention in particular many of Severi's results as well as the results of our first part. In the sequence, unless otherwise stated, in speaking of an Abelian variety, it will always be under-

* A birational transformation of the first kind of V_p is defined by equations such as

$$w_i = u_i + \text{const.} \quad (i = 1, 2, \cdots, p).$$

stood that we mean the variety of rank one without singularities in point to point correspondence without exception with U_{2p}, and it is this variety which we shall designate by V_p.

§ 2. Connectivity of varieties of rank one

52. Let now $u_1, u_2, \cdots, u_p$ be the variables corresponding to Ω and consider the generalized cube U_{2p} as defined by the relations

$$u_i = \sum_{\mu=1}^{2p} t_\mu \omega_{i\mu} \qquad (i = 1, 2, \cdots, p),$$

where the (t)'s describe the interval $0 \cdots 1$, end points included. U_{2p} will have for s-dimensional elements, the aggregates of points obtained when $2p - s$ of the (t)'s are equal to zero or one and the others vary. Two elements composed of congruent points modulo the periods are homologous. Hence, a system of $\binom{2p}{s}$ s-dimensional elements not congruent to each other form a minimum base for all elements of the same dimensionality. Besides, every one of them represents a closed s-dimensional manifold, that is, an s-cycle, and as these cycles are independent, we shall have a minimum base for s-cycles composed of independent cycles. Hence, for U_{2p}, and therefore for V_p, $R_s = \binom{2p}{s}$, $\sigma_s = 1$. In particular, $R_2 = p(2p-1)$, $\sigma_1 = \sigma = 1$. As a verification for hyperelliptic surfaces, the values $\rho_0 = 5$, $\rho = 1$, were given by Picard, and indeed, $R_2 = 6 = \rho_0 + \rho$.

53. We shall attack the same problem by a slightly different method, which will be found very useful below.

Let us designate by $1, 2, \cdots, 2p$, the edges of U_{2p}, abutting on the origin, and sense each of them in such manner that starting from the origin the direction of advancement be positive. The face (μ, ν) will be sensed by sensing its periphery so that the edge (μ) be a positive segment of it. We then have $(\mu, \nu) \sim -(\nu, \mu)$. From there we can pass to the sensing of a 3-dimensional face (μ, ν, π), etc. We are after all merely dealing here with Heegaard's "sensed corners".*

To each combination of indices, $i_1, i_2, \cdots, i_s$ correspond two opposite s-dimensional elements. Let M_s be an analytical s-cycle. Its projection on $(i_1, i_2, \cdots, i_s)$ is composed of that element counted several times. *I say that if we project it each time on only one of the elements corresponding to the indices $i_1, i_2, \cdots, i_s$, M_s is homologous to the sum of its projections.* Let us cut up M_s, as we may, into a sum of elements homologous to a hypersphere, then project one of these, M_s', as well as its boundary M_{s-1} upon $(i_1, i_2, \cdots, i_s)$. This will be done by passing a space S_{2p-s} through an arbitrary point A of M_s'

*Bulletin de la Société Mathématique de France, vol. 44 (1916), pp. 161–242.

and taking its intersection B with $(i_1, i_2, \cdots, i_s)$. An arbitrary line (straight or otherwise) joining A to B, will be called a projecting line of A. It is in no wise necessary that this projecting line be in the S_{2p-s}, but only that in some manner it should be uniquely and continuously defined for all points A.

By continuous deformation we may reduce M_s' to its projection M_s'' provided we replace it in M_s by this projection increased by the s-dimensional manifold M_s''' generated by the projecting lines of M_{s-1}. The manifold $M_s' + M_s''' - M_s''$ will form an s-cycle $\overline{M}_s$, reducible by deformation to a point, hence the conclusion: If P is an S_{2p-s} of the S_{2p} which contains U_{2p}, Poincaré's character belonging to $\overline{M}_s$ and P will be $(\overline{M}_s P) = 0$. By taking in particular for P a space normal to $(i_1, i_2, \cdots, i_s)$ it is seen that the projection of $\overline{M}_s$ on $(i_1, i_2, \cdots, i_s)$ is composed of mutually opposite elements. Hence, finally, when M_s' is replaced in M_s by $M_s'' - M_s'''$, the projections on the s-dimensional elements of U_{2p} are not changed. Proceeding similarly with all the s-dimensional elements such as M_s' of which M_s is composed, we shall succeed in replacing finally this cycle by $(i_1, i_2, \cdots, i_s)$ counted a certain number of times and an s-cycle whose projection on $(i_1, i_2, \cdots, i_s)$ has less than s dimensions while on any other s-dimensional element, the projection is the same as for M_s. We may reason similarly with the part of this new cycle exterior to $(i_1, i_2, \cdots, i_s)$ relatively to an element upon which it has an s-dimensional projection and so on, so that finally M_s will have been replaced by the sum of its projections. *The theorem is therefore proved.*

Remark. The proof holds also when we consider the projections on elements derived from those such as $(i_1, i_2, \cdots, i_s)$ by translation.

The s-cycles are equal to sums of multiples of the cycles $(i_1, i_2, \cdots, i_s)$ which therefore form a minimum base. To establish the independence of the cycles of this base, it is sufficient to remark with Picard, that the integral $\int\int\cdots\int dt_{i_1} dt_{i_2} \cdots dt_{i_s}$ has a period $+1$ relatively to $(i_1, i_2, \cdots, i_s)$ and 0 relatively to any other cycle. We have thus a system of $\binom{2p}{s}$ integrals with a period matrix relatively to the cycles in question of rank equal to the number of these periods. As these integrals have no periods relatively to the cycles homologous to zero, the $\binom{2p}{s}$ cycles thus obtained are independent and form a minimum base, hence again $R_s = \binom{2p}{s}$, $\sigma_s = 1$.

54. The s-uple integrals of the first kind of V_p, as is well known for $p = 2$ and easily proved for any p, are all linear combinations of the integrals

$$\int\int\cdots\int du_{j_1} du_{j_2} \cdots du_{j_s}.$$

Their number is therefore $i_s = \binom{p}{s}$. To say that there is a certain number of s-cycles with periods of integrals of the first kind all zero is therefore the same as to say that there are as many linear relations with integral coefficients

between the determinants of order s derived from the array

$$\begin{matrix} \omega_{j_1,1} & \omega_{j_1,2} & \cdots & \omega_{j_1,2p} \\ \omega_{j_2,1} & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \omega_{j_s,1} & \cdot & \cdots & \omega_{j_s,2p}, \end{matrix}$$

the coefficients being independent of the indices $j_1, j_2, \cdots, j_{2p}$.

In the case $s = 2$, the number of these independent relations is precisely the number $1 + k$ of alternate Riemann forms belonging to Ω. We have therefore for V_p according to Part I, $\rho \leqq 1 + k$. The consideration of intermediary functions will allow us to show that $\rho \geqq 1 + k$. Assuming this result, for the present, we have then $\rho = 1 + k$. In other words, *every two-cycle of V_p without periods of integrals of the first kind, is algebraic.* For $p = 2$, this has already been established by Bagnera and de Franchis. Thus, the theory of Part I leads us naturally to the consideration of the alternate Riemann forms of Ω.

55. Let us reduce Ω to the canonical matrix A. In general, there will be no other relations between the periods of the unique p-uple integral of the first kind of V_p than the following: Let

$$|a_{i_\alpha, j_\beta}|, \qquad |a_{j_\beta, i_\alpha}| \qquad (\alpha, \beta = 1, 2, \cdots, s)$$

be two minors of the determinant $|a_{jh}|$ $(j, h = 1, 2, \cdots, p)$, symmetrical relatively to the principal diagonal, then denote for the present by $\omega_{i\mu}$ the term of the matrix A at the intersection of the ith row and μth column. To the first of our minors corresponds the following determinant of order p derived from A:

$$D = \begin{vmatrix} \omega_{1h_1}, & \omega_{1h_2}, & \cdots, & \omega_{1h_{p-s}}, & a_{1j_1}, & a_{1j_2}, & \cdots, & a_{1j_s} \\ \omega_{2h_1}, & \omega_{2h_2}, & \cdots, & \omega_{2h_{p-s}}, & a_{2j_1}, & a_{2j_2}, & \cdots, & a_{2j_s} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \omega_{ph_1}, & \cdots, & \cdots, & \omega_{ph_{p-s}}, & a_{pj_1}, & \cdots, & \cdots, & a_{pj_s} \end{vmatrix},$$

where the (h)'s are integers in increasing order such that $h_1, h_2, \cdots, h_{p-s}$, $j_1, j_2, \cdots, j_s$, form in some order the sequence, $1, 2, \cdots, p$. Similarly there corresponds to the other minor a determinant of order p, D', derived from A by adjunction of certain columns of indices $k_1, k_2, \cdots, k_{p-s}$, at most equal to p. One verifies at once that $e_{h_1} \cdot e_{h_2} \cdots e_{h_{p-s}} \cdot D = e_{k_1} \cdot e_{k_2} \cdots e_{k_{p-s}} \cdot D'$. When A is as general as possible, every linear relation with integral coefficients existing between the determinants of order p derived from A reduces to a combination of those of that type which result immediately from the fact that $|a_{jh}|$ $(j, h = 1, 2, \cdots, p)$ is a symmetrical determinant. Their number is equal to half the number of non-symmetrical minors derived from the pre-

ceding determinant, that is to

$$\frac{1}{2}\sum_{j=1}^{p}\binom{p}{j}\left[\binom{p}{j}-1\right]=\frac{1}{2}\binom{2p}{p}-2^{p-1}.$$

This is the number of p-cycles with zero periods for the p-uple integral of the first kind of V_p when the variety is as general as possible.

Let us start from the relation

$$(1+i)^{2p}=2^p i^p=\sum_{j=0}^{p}\binom{2p}{j}i^j.$$

By considering separately the two cases where p is even or odd, we find that

$$\frac{1}{2}\binom{2p}{p}-2^{p-1}=R_{p-2}-R_{p-4}+R_{p-6}-\cdots,$$

and therefore according to Part I, $\rho_p=0$.

A similar though somewhat more complicated discussion which we have not carried out in detail leads no doubt to $\rho_s=0$. Thus *the numbers ρ_s of the most general Abelian variety of rank one are all zero.*

For a special V_p the number of s-cycles with zero periods for the integrals of the first kind may exceed the above. Let generally,

$$k_s+R_{s-2}-R_{s-4}+\cdots$$

be this number, $k_s\geqq 0$. The integer k_s may be called the s-dimensional index of singularity of V_p or Ω. We always have

$$\rho_s\leqq k_s,\qquad \rho_s^0\geqq\binom{2p}{s}-\binom{2p}{s-2}-k_s.$$

We may of course introduce an s-dimensional index of multiplication. All these indices would no doubt be useful for the classification of Abelian varieties and many of the propositions given by Scorza for $s=2$ could be extended to them but we shall not discuss this any further.

§ 3. Intermediary functions

57. An entire function $\phi(u_1, u_2, \cdots, u_p)$ belonging to a matrix Ω with p rows and $2p$ columns is said to be an intermediary function if

$$\phi(u+\omega_\mu)=e^{-2\pi i(\sum_{j=1}^{p}\alpha_{j\mu}u_j+\beta_\mu)}\cdot\phi(u)\qquad(\mu=1,2,\cdots,2p).$$

By comparing the two possible values for $\phi(u+\omega_\mu+\omega_\nu)$ the following equations of condition are obtained:

$$\sum_{j=1}^{p}(\alpha_{j\mu}\omega_{j\nu}-\alpha_{j\nu}\omega_{j\mu})=m_{\mu\nu}\qquad(\mu,\nu=1,2,\cdots,2p).$$

where the (m)'s are integers. Since $m_{\mu\nu} = -m_{\nu\mu}$ the form

$$F = \sum_{\mu,\nu=1}^{2p} m_{\mu\nu} x_\mu y_\nu$$

is an alternate form with integral coefficients. We shall call it the *fundamental form* belonging to ϕ. It will play a very important part in the sequence.

58. The second derivatives of $\log \phi$ are meromorphic periodic functions belonging to Ω. We shall assume that they are effectively $2p$-ply periodic, which is permissible, for otherwise we could replace Ω by the matrix of genus $< p$, formed by the primitive periods. Ω will then be a Riemann matrix of genus p.

If ϕ is a function which vanishes nowhere, the second derivatives of $\log \phi$ are entire periodic functions and therefore they are constants, hence ϕ is of the form $e^{G(u)}$, where G is a quadratic polynomial in the (u)'s. Let us assume that ϕ is not of this type. The second derivatives of $\log \phi$ will then be of type θ_m/θ'_m and there will be a hypersurface E of V_p determined by $\phi = 0$, or, as we shall say, cut out by ϕ. By a θ_m we mean a θ-function belonging to a canonical matrix A equivalent to Ω. In terms of the (u)'s it is a function

$$\theta_m(\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_p u_p);$$

in reality an intermediary function derived from a θ.

The hypersurface cut out by θ'_m is composed of E and of another hypersurface E' upon which θ_m vanishes also. As θ_m, θ'_m, cut out algebraic hypersurfaces, their common part E' is also algebraic. Hence, E, the residue of an algebraic hypersurface with respect to another, is itself algebraic and therefore *any intermediary function cuts out in V_p an algebraic hypersurface.*

59. For the sequence, it is very important to show that an arbitrary intermediary function is always reducible to a θ by a linear change of variables. This reduction has been very simply effected for $p = 2$ by Humbert, Bagnera and de Franchis. Humbert's method may be extended to any p, but as it consists in taking Ω always in the canonical form, we do not obtain thus in any simple manner the relationship between fundamental and principal forms. As to the method of Bagnera and de Franchis, we have not succeeded in extending it. The difficulty consists in showing that a certain form is principal. The method to be followed here, completely different from that of these authors, seems to present considerable interest in itself and probably will be useful in other applications as well.

This method consists in the following: We shall obtain the expression of the algebraic cycle (E^{p-1}) in terms of the cycles (μ, ν), and from the expression in question, we shall deduce that the *inverse* of the fundamental form is a principal form of Riemann.

60. In the first place, the hypersurface (E) itself is a $(2p-2)$-cycle. We shall first seek the expression of this cycle (E) in terms of the $p(2p-1)$ fundamental cycles. Let $(E) \sim \Sigma m_{i_1 i_2 \cdots i_{2p-2}} (i_1, i_2, \cdots, i_{2p-2})$. In the sum at the right, only one of the cycles corresponding to a given combination of indices must be taken. We shall agree to take always the cycle for which the (i)'s are in increasing order. The question is to evaluate the coefficients in the homology. We shall see that if E is irreducible, a hypothesis which will be made until further notice, (E) considered as a manifold entirely in U_{2p} is sensed everywhere in the same manner with respect to the $(2p-2)$ dimensional elements of U_{2p}, which translates itself into the fact that its projections on $(i_1, i_2, \cdots, i_{2p})$ do not include any $(2p-2)$ dimensional elements which destroy each other. It will be necessary then, first to determine that sense, then the number of times that the projection on $(i_1, i_2, \cdots, i_{2p-2})$ covers it up.

61. We must first examine a little closer the notion of sense. Let there be given in an S_q a system of q directed rectangular axes and corresponding variables $t_1, t_2, \cdots, t_q$ and in that space an analytical manifold of $k < q$ dimensions, M_k, without any singular points. We wish to define what is meant by the sensing of that element with respect to the S_k defined by the equations $t_{i_1} = t_{i_2} = \cdots = t_{i_{q-k}} = 0$, which we will designate by $(i_{q-k+1}, i_{q-k+2}, \cdots, i_q)$, it being understood that $t_{i_{q-k+1}}, \cdots, t_{i_q}$ are variable in that space.

Let M'_{q-k} be an S_{q-k} transverse to M_k and passing through one of its points A and take a system of q axes, of which $q-k$, $As_1, As_2, \cdots, As_{q-k}$ are in M'_{q-k} and k others $As_{q-k+1}, As_{q-k+2}, \cdots, As_q$ are in M_k. More precisely the coordinates of any point of M_k are, in the vicinity of A, analytical functions of certain variables s_{q-k+i} $(i = 1, 2, \cdots, k)$. We may define the "axes in M_k" as the tangents at A to the lines $ds_{q-k+i} \neq 0$, $ds_{q-k+j} = 0$ $(j \neq i)$, sensed positively in the direction of increreasing (s)'s.—Assume first that the axes t_{i_k} are congruent to those just defined, i.e. if t'_h are the variables for this second set, that there exists a continuous series of infinitesimal transformations of the group with parameters a_{ik}, b_i,

$$t'_i = \sum_{k=1}^{q} a_{ik} t_{i_k} + b_i, \qquad |a_{ik}| = +1 \quad (i, k = 1, 2, \cdots, q)$$

reducing the first axes to the second. This continuous series of transformations defines a displacement in S_q. The Jacobian is

$$\frac{D(s_1, s_2, \cdots, s_q)}{D(t_{i_1}, t_{i_2}, \cdots, t_{i_q})} = +1$$

If there exists such a displacement for which the Jacobian

$$\frac{D(t'_1, t'_2, \cdots, t'_{q-k})}{D(t_{i_1}, t_{i_2}, \cdots, t_{i_{q-k}})}$$

changes its sign an even number of times, we shall say that M_k is sensed positively with respect to the initial space, $(i_{q-k+1}, \cdots, i_q)$. In such a displacement, a sufficiently small k-dimensional element within the displaced space $(i_{q-k+1}, \cdots, i_q)$ is never projected within its initial position into an element of $< k$ dimensions or is so an even number of times. Finally, the product

$$\frac{D(s_1, s_2, \cdots, s_{q-k})}{D(t_{i_1}, t_{i_2}, \cdots, t_{i_{q-k}})} \cdot \frac{D(s_1, s_2, \cdots, s_q)}{D(t_{i_1}, t_{i_2}, \cdots, t_{i_q})} > 0.$$

If on the contrary the sign considered above changes an odd number of times—and it is easy to show that its parity is perfectly defined—we shall say that the sense in question is negative. The product of the two Jacobians is then negative.

If the axes (s) and (t) are not congruent, we compare M_k to the S_k corresponding to the indices $i_2, i_1, i_3, \cdots, i_q$ which is opposed to $(i_{q-k+1}, \cdots, i_q)$ and we define the sense as being opposite to that then obtained. We see then that the sense is always given by the sign of the Jacobian product, which may therefore be used as definition of this sense. The axes (s) will be called intrinsic axes of M_k.

62. Let us return to our problem. To show first that (E) has an invariant sense relatively to $(i_3, i_4, \cdots, i_{2p})$ it is sufficient to establish that if $s_1, s_2, \cdots, s_{2p}$ is a system of intrinsic axes and s_1, s_2, the variables belonging to the transverse plane the Jacobians $D(s_1, s_2)/D(t_{i_1}, t_{i_2})$ vanish only on a manifold of $(2p-4)$ dimensions at most, of (E). Let

$$\phi = \phi' + i\phi'', \qquad u_j = u_j' + iu_j'',$$

where $\phi', \phi'', u_j', u_j''$ are real, and take as coördinates s_1, s_2, two distinct linear combinations of ϕ', ϕ''. The question is reduced to showing then that the Jacobian $D(\phi', \phi'')/D(t_1, t_2)$, for example, vanishes only on a $(2p-4)$-dimensional manifold of (E). But the left hand side is a linear combination with constant coefficients of products of terms such as $\partial\phi'/\partial u_j'$, $\partial\phi'/\partial u_j''$, $\partial\phi''/\partial u_j'$, $\partial\phi''/\partial u_j''$, that is, by virtue of classical relations, of terms $\partial\phi/\partial u_j$. It is therefore an entire function of $u_1, u_2, \cdots, u_p$ and the dimension of the manifold in question is at most $2p-4$.

It follows from this that $m_{i_3 i_4 \cdots i_{2p}}$ has the sign of the product

$$\frac{D(t_{i_1}, t_{i_2})}{D(s_1, s_2)} \cdot \frac{D(t_{i_1}, t_{i_2}, \cdots, t_{i_{2p}})}{D(s_1, s_2, \cdots, s_{2p})}.$$

But the second factor is equal to $(-1)^n D(t_1, t_2, \cdots, t_{2p})/D(s_1, s_2, \cdots, s_{2p})$ where n is the number of transpositions of the permutation $\left(\begin{smallmatrix} i_1, & i_2, & \cdots, & i_{2p} \\ 1, & 2, & \cdots, & 2p \end{smallmatrix}\right)$. Finally, we can always choose the (s)'s in such a way that the coefficient of

$(-1)^n$ will be positive. In these conditions $m_{i_3 i_4 \cdots i_{2p}}$ will have the sign of $(-1)^n D(t_{i_1}, t_{i_2})/D(s_1, s_2)$.

To determine the absolute value of $m_{i_3 i_4 \cdots i_{2p}}$, we remark that the number of times that the projection of an (E) on an $(i_3, i_4, \cdots, i_{2p})$ covers it up, is equal to the absolute value of

$$\frac{1}{2\pi i}\int d \log \phi$$

taken over the positive contour of (i_1, i_2). The value as found by an elementary integration is* $\sum_{j=1}^{p} (\alpha_{j i_1} \omega_{j i_2} - \alpha_{j i_2} \omega_{j i_1}) = m_{i_1 i_2}$. Now let us take in the transverse plane, a circuit ζ surrounding its point of incidence and such that

$$\frac{1}{2\pi i}\int_{\zeta} d \log \phi = +1.$$

We shall assume the axes s_1, s_2, so chosen that ζ is sensed positively in the direction s_1, s_2.

Let ζ' be the projection of ζ on (i_1, i_2) when the point of incidence of the transverse plane comes in one of the points where (E) cuts (i_1, i_2). We have

$$\frac{1}{2\pi i}\int_{\zeta} d \log \phi = \frac{1}{2\pi i}\int_{\zeta_1} d \log \phi = +1.$$

Hence the integral taken over the contour of (i_1, i_2) in the sense from i_1 towards i_2, is positive if ζ' and the contour have the same sense, negative in the contrary case. Therefore

$$m_{i_1 i_2} \frac{D(t_{i_1}, t_{i_2})}{D(s_1, s_2)} > 0,$$

and finally $m_{i_3 i_4 \cdots i_{2p}} = (-1)^n m_{i_1 i_2}$. If n' corresponds to the indices $i_2, i_1, \cdots, i_{2p}$ we have $(-1)^n = -(-1)^{n'}$, $(-1)^n m_{i_1 i_2} = (-1)^{n'} m_{i_2 i_1}$, and we can decide without inconvenience to take $i_1 < i_2$ since we must choose only one of these combinations. In assuming, as we already had occasion to state, $i_3 < i_4 < \cdots < i_{2p}$, n will be the number of transpositions which bring i_1, i_2, into the position $1, 2$. Finally then

$$(E) \sim \sum (-1)^n m_{i_1 i_2} (i_3, i_4, \cdots, i_{2p}).$$

63. Let us show that with a suitable convention nothing is changed, even if E is reducible.

I say first, that two arbitrary hypersurfaces, (E'), (E'') have two sides sensed alike with respect to all the $(i_3, i_4, \cdots, i_{2p})$. For, taking always a

* Poincaré, as I have found since writing the above, has already used analagous considerations in a memoir of the Acta mathematica, vol. 26 (1902), pp. 43–98.

representation analogous to (5) of No. 50 for V_p, there exists a polynomial $F(x_1, x_2, \cdots, x_s)$ vanishing on E' and E''. Replacing the (x)'s by the (θ)'s, we see that E', E'', are part of an irreducible hypersurface cut out by a certain θ. Hence (E'), (E''), have an invariant sense at all their points. Moreover, there exists an algebraic variety of the S_{s-1}, containing V_p, cutting out on V_p an irreducible hypersurface, G, tangent to E', E'' in two ordinary points, A, B. If we prefer, we may say that there is a suitable θ cutting out G. Let us now take on (E'), (E''), (G), intrinsic coördinates with the corresponding axes congruent to each other, and let s'_j, s''_j, s_j be these coördinates. The senses with respect to $(i_2, i_4, \cdots, i_{2p})$ of (E'), (G) in A and of (E''), (G) in B will be the same or opposite according as the Jacobians $D(s'_1, s'_2)/D(s_1, s_2)$, $D(s''_1, s''_2)/D(s_1, s_2)$ are positive or negative, the first in A and the second in B. As these signs do not depend upon the (i)'s, our affirmation follows.

The preceding discussion makes it possible to define a typical sensing for algebraic hypersurfaces of V_p to be taken as positive, and this we shall do in the future.

Let us assume that (E'), (E''), are two irreducible parts of the hypersurface (E) cut out by ϕ and that they intersect in a point, A, ordinary for both. Through A we draw a plane parallel to (i_1, i_2) wherein we trace a small circuit ζ surrounding A. By attributing to ζ' a suitable direction, we shall have $\int_\zeta d \log \phi = +\, 2 \cdot 2\pi i$. Through a point near A, let us draw a plane transverse to (E'), then surround its point of incidence with a small circuit ζ', avoiding (E'') and sensed in such a way that

$$\int_{\zeta'} d \log \phi = 2\pi i.$$

Let ζ'' be an analogous circuit for (E''). As $\int_\zeta d \log \phi = \int_{\zeta'} + \int_{\zeta''}$, ζ', ζ'' are sensed similarly with respect to all the (i_1, i_2). If, therefore, we desire once for all to take for every hypersurface only the cycle formed by its positive side, the Jacobians $D(t_{i_1}, t_{i_2})/D(s_1, s_2)$ will still have the same sign at all points of (E) provided the intrinsic axes are congruent at all points. These signs will always be those of the coefficients $m_{i_1 i_2}$, and our reasoning still holds, leading again to the same homology as previously.

Let us assume, finally, that (E'), (E''), have no simple points in common, and let ψ be an intermediary function cutting out a hypersurface G, which meets E', E'' in two ordinary points, A', A''. By reasoning as we have just done, with $\phi\psi$ taking now the place of ϕ, and comparing E' and E'' with G, we show at once that we can always arrange matters so that the Jacobians $D(t_{i_1}, t_{i_2})/D(s_1, s_2)$ have the same sign on (E') and (E''), the corresponding intrinsic axes being always assumed congruent. The rest can be completed as previously.

Remark. An immediate consequence of the similar sensing of the hypersurfaces of V_p is that the signs of the coefficients $m_{i_1 i_2}$ depend only upon the indices *but not upon the fundamental form considered.* The sign of $(-1)^n m_{i_1 i_2}$ indicates the sensing of the algebraic hypersurfaces of V_p relatively to $(i_3, i_4, \cdots, i_{2p})$.

64. It is clear that, in the same manner as above for a $2p-2$ dimensional element, the sensing of a $2p-4$ dimensional element with respect to $(i_5, i_6, \cdots, i_{2p})$ can be considered as determined by the sign of the product

$$\frac{D(t_{i_1}, t_{i_2}, t_{i_3}, t_{i_4})}{D(s_1, s_2, s_3, s_4)} \cdot \frac{D(t_{i_1}, t_{i_2}, \cdots, t_{i_{2p}})}{D(s_1, s_2, \cdots, s_{2p})},$$

where the coördinates s_1, s_2, s_3, s_4 belong to the transverse S_4 and the others belong to the element itself.

We can show next that the image in U_{2p} of an irreducible $p-2$ dimensional algebraic subvariety of V_p is a $2p-4$ dimensional manifold sensed relatively to the $(i_5, i_6, \cdots, i_{2p})$, in a manner invariant in all its points and independent of the subvariety chosen.

Let us consider finally several such subvarieties belonging to the intersection of two algebraic hypersurfaces E_1, E_2. At all their points we can take intrinsic coördinates, $s_1, s_2, \cdots, s_{2p}$, such that s_1, s_2 belong to the plane transverse to (E_1), s_3, s_4 to the plane transverse to (E_2), and such that, moreover, the Jacobians

$$\frac{D(t_1, t_2, \cdots, t_{2p})}{D(s_1, s_2, \cdots, s_{2p})}, \frac{D(t_{i_1}, t_{i_2})}{D(s_1, s_2)}, \frac{D(t_{i_1}, t_{i_2})}{D(s_3, s_4)}$$

should be, the first equal to one, and the other two of invariant sign at all points of the intersection of (E_1) with (E_2). This is equivalent to associating in a definite way, (E_1), (E_2), in their common points. The known identity

$$\frac{D(t_{i_1}, t_{i_2}, t_{i_3}, t_{i_4})}{D(s_1, s_2, s_3, s_4)} = \sum \pm \frac{D(t_{i_1}, t_{i_2})}{D(s_\alpha, s_\beta)} \cdot \frac{D(t_{i_3}, t_{i_4})}{D(s_\gamma, s_\delta)}$$

shows that we change the sense of the intersection whenever we change the sense of one of the hypersurfaces but not when we change that of both. We shall agree always to associate the sides of (E_1), (E_2) which have the same sense. The side thus obtained for their intersection will be said to be its positive side. The sum of the irreducible parts similarly sensed will be what we shall call the intersection $(E_1 E_2)$. The following are two of its properties: (*a*) The cycles $(E_1 E_2)$ and $(E_2 E_1)$ are identical; (*b*) let there be two cycles Δ_1, Δ_2, nowhere sensed in opposition to (E_1), (E_2), and respectively reducible to these two cycles by a deformation, during which they never acquire a common $2p-3$ dimensional part. We may define their common $(2p-4)$-cycle $\Delta_1 \Delta_2$ as we have done for (E_1), (E_2), and this cycle is homologous to $(E_1 E_2)$.

65. Let us designate for the present by $(i_1, i_2, \cdots, i_s)$ not merely an element forming part of the boundary of U_{2p} but more generally any element which may be derived from it by a translation parallel to an edge—such an element forming of course a homologous cycle.

The hypersurfaces E_1, E_2, are cut out by intermediary functions belonging to two fundamental forms

$$F_1 = \sum m^1_{\mu\nu}\, x_\mu\, y_\nu\,, \qquad F_2 = \sum m^2_{\mu\nu}\, x_\mu\, y_\nu\,.$$

We can take for cycles Δ_1, Δ_2, the following:

$$\Delta_1 = \sum (-1)^n\, m^1_{i_1 i_2}\, (i_3, i_4, \cdots, i_{2p})\,, \quad \Delta_2 = \sum (-1)^n\, m^2_{i_1 i_2}\, (i''_3, i''_4, \cdots, i''_{2p})\,,$$

where at the right the cycles are so chosen that Δ_1, Δ_2 do not have any $(2p-3)$-dimensional manifold in common.

Owing to the large degree of arbitrariness in the definition of the projecting lines in No. 53, we may first reduce (E_1) to Δ_1, then (E_2) to Δ_2 in such a manner that during the deformation the two cycles never acquire a common $(2p-3)$-dimensional manifold. The property (b) is then applicable here and we shall have $(\Delta_1\, \Delta_2) \sim (E_1\, E_2)$.

The question is therefore reduced to the determination of the $(2p-4)$-dimensional cycles common to the $(i_3, i_4, \cdots, i_{2p})$. Now consider the elements $(i_3, i_4, \cdots, i_{2p})$, $(i''_3, i''_4, \cdots, i''_{2p})$. They are respectively represented by two systems of equations

$$x_{i_1} = \text{const.}, \qquad x_{i_2} = \text{const.}; \qquad\qquad x_{i'_1} = \text{const.}, \qquad x_{i'_2} = \text{const.},$$

where the two sequences $i_1, i_2, \cdots, i_{2p}$ and $i'_1, i'_2, \cdots, i'_{2p}$ form each in a certain order the sequence of integers, $1, 2, \cdots, 2p$. These equations will be compatible if and only if the four indices, i_1, i_2, i'_1, i'_2 are all different. We will then have intersection of the cycles $(i_3, i_4, \cdots, i_{2p})$, $(i''_3, i''_4, \cdots, i''_{2p})$ only if all their indices except two are the same. Let i_α, i_β be those of the first which do not belong to the second, i''_γ, i''_δ those of the second which do not belong to the first, and n, n' the numbers of transpositions bringing these pairs of indices into the position $1, 2$, from their right place in the sequence $1, 2, \cdots, 2p$. We can replace (E_1), (E_2), by the sums of homologous cycles. In the one belonging to (E_1) we have the term

$$(-1)^{n'}\, m_{i'_\gamma i'_\delta}\, (i_3, i_4, \cdots, i_{2p})$$

and in that belonging to (E_2), the term $(-1)^n\, m_{i_\alpha i_\beta}\, (i''_3, i''_4, \cdots, i''_{2p})$, and in no other terms of the sum do the same cycles appear. Let $j_5, j_6, \cdots, j_{2p}$ be the common indices. These two terms can be replaced by

$$(-1)^{n+n'}\, m_{i'_\gamma i'_\delta}\, (i_\alpha, i_\beta, j_5, \cdots, j_{2p})$$

and $(-1)^{n+n'} m_{i_\alpha i_\beta}(i''_\gamma, i''_\delta, j_5, \cdots, j_{2p})$ respectively. Their intersection is composed of the cycle

$$m^2_{i_\alpha i_\beta} m^1_{i'_\gamma i'_\delta} \frac{D(t_{i_\alpha}, t_{i_\beta}, t_{i'_\gamma}, t_{i'_\delta}, t_{j_5}, \cdots, t_{j_{2p}})}{D(t_1, t_2, \cdots, t_{2p})} (j_5, j_6, \cdots, j_{2p}),$$

the Jacobian being introduced as above for reasons of sensing. This term is of the type

$$(-1)^n m^1_{i_1 i_2} m^2_{i_3 i_4} (i_5, i_6, \cdots, i_{2p}),$$

where n is always the same number and can be taken to be equal to the sum of the transpositions bringing the pairs i_1, i_2 and i_3, i_4 each from their proper places in the sequence $1, 2, \cdots, 2p$ into the position $1, 2$. If we assume each of the three systems of indices $i_1, i_2; i_3, i_4; i_5, i_6, \cdots, i_{2p}$, in increasing order, we shall have

$$(E_1 E_2) \sim \sum (-1)^n m^1_{i_1 i_2} m^2_{i_3 i_4} (i_5, i_6, \cdots, i_{2p})$$

and in particular if we decide always to take $i_1 < i_3$

$$(E^2) \sim 2\sum (-1)^n m_{i_1 i_2} m_{i_3 i_4} (i_5, i_6, \cdots, i_{2p}).$$

This can be generalized at once and we shall have with conventions similar to those already made

$$(E_1 E_2 \cdots E_s) \sim \sum (-1)^n m^1_{i_1 i_2} m^2_{i_3 i_4} \cdots m^s_{i_{2s-1} i_{2s}} (i_{2s+1}, i_{2s+2}, \cdots, i_{2p})$$

$$(E^s) \sim s! \sum (-1)^n m_{i_1 i_2} m_{i_3 i_4} \cdots m^s_{i_{2s-1} i_{2s}} (i_{2s+1}, i_{2s+2}, \cdots, i_{2p}).$$

It is of course understood that the various irreducible parts of $(E_1 E_2 \cdots E_s)$ are everywhere sensed alike.*

66. The two most interesting cases are $s = p$ and $s = p - 1$. In the first case we obtain, except for the sign, $[E_1 E_2 \cdots E_p]$ which is the number of zeros common to p intermediary functions. In particular†

$$\pm [E^p] = p! \sum (-1)^n m_{i_1 i_2} m_{i_3 i_4} \cdots m_{i_{2p-1} i_{2p}} = p! \pi,$$

where the quantity π is the *pfaffian* of the skew symmetric determinant $|m_{jk}|$ $(j, k = 1, 2, \cdots, 2p)$ of the fundamental form F.

For $s = p - 1$ we obtain *the expression for the algebraic two-cycle*:

$$(E^{p-1}) \sim (p-1)! \sum (-1)^n m_{i_1 i_2} m_{i_3 i_4} \cdots m_{i_{2p-3} i_{2p-2}} (i_{2p-1}, i_{2p}).$$

The coefficient of (i_{2p-1}, i_{2p}) in the sum multiplied by π is equal to the coeffi-

* (E^s) is actually a $(2p - 2s)$-cycle, for the functions $\phi(u - e)$ cut out hypersurfaces of $\{E\}$, and s of them with the (e)'s arbitrary will intersect in a $2p - 2s$ dimensional manifold, as may be shown for example by recurrence.

† For ordinary θ's this reduces to a classical formula due to Poincaré.

cient $M_{i_{2p-1}i_{2p}}$ of $m_{i_{2p-1}i_{2p}}$ in the expansion of the determinant of F. Hence, finally

$$\pi(E^{p-1}) \sim (p-1)! \sum M_{\mu\nu}(\mu, \nu) \qquad (\mu < \nu).$$

67. Since (E^{p-1}) is algebraic, the corresponding periods of the integrals of the first kind of V_p are zero, hence $\Phi = \sum M_{\mu\nu} x_\mu y_\nu$, which up to a numerical factor is the *inverse* of F, is an alternate Riemann form of Ω. We shall see that it is a principal form of Ω or else is such a form changed in sign.*

Assume, indeed, first that (E^{p-1}) is irreducible. We mean thereby, explicitly, that there exist $p-2$ hypersurfaces of the same algebraic system as E, whose intersection with E is an irreducible curve. Let ζ be the contour making (E^{p-1}) simply connected, and let $X = x + iy$ be one of the point coördinates on (E^{p-1}). Finally, set

$$u = u' + iu'' = \sum_{j=1}^{p} \lambda_j u_j; \qquad \xi_\mu + i\eta_\mu = \sum_{j=1}^{p} \lambda_j \omega_{j\mu}.$$

We have, according to Riemann,

$$\iint_{a(E^{p-1})} \left[\left(\frac{\partial u'}{\partial x} \right)^2 + \left(\frac{\partial u'}{\partial y} \right)^2 \right] dxdy = \int_\zeta u' \, du'' > 0.$$

But by means of a classical transformation of the first integral

$$\begin{aligned} \int_\zeta u' \, du'' &= \iint_{a(E^{p-1})} \frac{D(u', u'')}{D(x, y)} \, dxdy = \iint_{a(E^{p-1})} du' \, du'' \\ &= \pm \frac{(p-1)!}{\pi} \sum M_{\mu\nu} \iint_{(\mu,\nu)} du' \, du'' \\ &= \pm \frac{(p-1)!}{\pi} \sum M_{\mu\nu} (\xi_\mu \eta_\nu - \xi_\nu \eta_\mu) > 0, \end{aligned}$$

which proves our affirmation in the case considered.

The signs $\pm$ come from the fact that it is only for one of the sides of (E^{p-1}) that the double integral will be positive.

Assume now that E^{p-1} is composed of several irreducible curves $C_1, C_2, \cdots, C_n$. The cycle (E^{p-1}) is composed of the sum of the cycles (C_j) all assumed sensed in the same manner. We know that the following condition will then be fulfilled: Let C be an arbitrary algebraic curve tangent to C_j at a simple point A and to C_h at a simple point B, then trace in a tangent plane at A and B, two small circuits ζ', ζ'' around these points. If we impose upon ζ', ζ'' directions corresponding to the positive circuits of C_j and C_h, they will both be sensed alike with respect to C. More precisely speaking,

* Since this was written the same result has been derived in a more direct and elegant manner by Castelnuovo. See Rendiconti dei Lincei, ser. 5, vol. 30 (1921), pp. 50–55.

we may consider a small positive circuit ζ of (C) starting from the interior of a small tube of axis ζ' (a tube of which the transverse dimensions are very small with respect to ζ'), then bring it into a similar position relatively to ζ'' without changing its sense. The integral $\int_\zeta u'\,du'' - \int_{\zeta''} u'\,du''$ will be at first very small with respect to each term of the difference, and similarly when we consider $\int_\zeta u'\,du'' - \int_{\zeta''} u'\,du''$ and the final position of ζ. Since, besides, the first integral does not change its sign, the two integrals $\int_{\zeta'}\ \int_{\zeta''}$ have the same sign. This sign will be that of every positive circuit bounding on (C_j) or (C_h) and we may assume that it is the sign $+$.

Let us draw in particular the contours ζ_j making the (C)'s simply connected. They bound on these manifolds, hence we can sense them. If we do this in the manner just defined, we shall then have $\int_{\zeta_1} du'\,du'' > 0$;

$$\therefore\ \sum \int_{\zeta_j} u'\,du'' = \sum \int\int_{(C_j)} du'\,du'' = \int\int_{\Delta(E^{p-1})} du'\,du'' > 0,$$

and the rest is ended as previously. Hence finally:

THEOREM. *The inverse of a non-singular fundamental form is up to the sign a principal form of* Ω.

Remark. If ϕ is of genus $p_1 < p$, we may, as we have already stated, reduce Ω to the form

$$\begin{Vmatrix} \Omega_1, & 0 \\ 0, & \Omega_2 \end{Vmatrix},$$

where Ω_1 is of genus p_1, ϕ being a function of the sole variables belonging to Ω_1. F will then be a fundamental form belonging to Ω_1, hence degenerate for Ω, and the inverse Φ of F considered as non-degenerate form of genus p_1, will be a principal form for Ω_1, and therefore will be a degenerate alternate form of Ω.

67. Before continuing with the reduction of intermediary forms, let us establish a generalization of Riemann's classical inequality. Its interest lies in the fact that it is the only one known to date for multiple integrals of the first kind.

Let $v_1, v_2, \cdots, v_s$ be distinct linear combinations of the variables $u_1, u_2, \cdots, u_p$, and $x_1, x_2, \cdots, x_s$, s arbitrary point coördinates on $E_1, E_2, \cdots, E_{p-s}$, then set $v_j = v_j' + iv_j''$, $x_j = x_j' + ix_j''$. By starting with the relations

$$\frac{\partial v_j}{\partial x_k} = \frac{\partial v_j'}{\partial x_k'} + i\frac{\partial v_j''}{\partial x_k'}, \qquad i\frac{\partial v_j}{\partial x_h} = \frac{\partial v_j'}{\partial x_h''} + i\frac{\partial v_j''}{\partial x_h''},$$

$$\frac{\partial \bar{v}_j}{\partial \bar{x}_k} = \frac{\partial v_j'}{\partial x_h'} - i\frac{\partial v_j''}{\partial x_k'}, \qquad -i\frac{\partial \bar{v}_j}{\partial \bar{x}_k} = \frac{\partial v_l'}{\partial x_h''} - i\frac{\partial v_j''}{\partial x_h''}$$

we find that

$$\frac{D(v_1', v_2', \cdots, v_s', v_1'', \cdots, v_s'')}{D(x_1', x_2', \cdots, x_s', x_1'', \cdots, x_s'')} = \left(-\frac{1}{2}\right)^s \left|\frac{D(v_1, v_2, \cdots, v_s)}{D(x_1, x_2, \cdots, x_s)}\right|^2$$

and therefore

$$\int\int \cdots \int_{(E_1 E_2 \cdots E_{p-s})} dv_1' \, dv_2' \cdots dv_s' \, dv_1'' \cdots dv_s'' \neq 0.$$

The sign of this multiple integral depends only upon the sensing of the (E)'s but not upon these hypersurfaces nor even upon V_p. Suppose in particular that V_p possesses p independent elliptic integrals which we shall still denote by $u_1, u_2, \cdots, u_p$ and take for hypersurfaces E_j, an hypersurface which is here algebraic, defined by

$$u_{s+j} = \text{const.} \qquad (j = 1, 2, \cdots, p - s).$$

The multiple integral is then reduced to the product by $(-1)^{\frac{s(s-1)}{2}}$ of s integrals of type

$$\int\int_{(E_1 E_2 \cdots E_{p-1})} du_1' \, du_1''$$

which have all the same sign. Hence

$$(-1)^{\frac{s(s-1)}{2}} \int\int \cdots \int_{(E_1 E_2 \cdots E_{p-s})} dv_1' \, dv_2' \cdots dv_s' \, dv_1'' \cdots dv_s''$$

is positive if s is even and has the sign of the double integral if s is odd. Let $\tau_{i_{2(p-s)+1} i_{2(p-s)+2} \cdots i_{2p}}$ be the period of the multiple integral with which we are dealing, with respect to $(i_{2(p-s)+1}, \cdots, i_{2p})$. The quantity

$$(-1)^{\frac{s(s-1)}{2}} \sum (-1)^n m^1_{i_1 i_2} m^2_{i_3 i_4} \cdots m^{p-s}_{i_{2(p-s)-1} i_{2(p-s)}} \tau_{i_{2(p-s)+1} \cdots i_{2p}}$$

is positive if s is even and has the same sign as for $s = 1$ if s is odd. This is the generalization which we had in view.

68. It is easy to show now that we can always transform Ω into a canonical matrix A in such a way that ϕ becomes, up to a quadratic exponential factor, a θ belonging to A. We can obviously assume that ϕ is of genus p.

Reduce Ω to a canonical matrix A in such a way that Φ becomes the form

$$\Phi' = \sum_{\mu=1}^{p} e_\mu (x_\mu y_{p+\mu} - x_{p+\mu} y_\mu).$$

The transformed of F is then

$$F' = m e_p \sum_{\mu=1}^{p} \frac{(x_\mu y_{p+\mu} - x_{p+\mu} y_\mu)}{e_\mu},$$

where m is up to the sign the greatest common divisor of the coefficients of F. Let $u_1', u_2', \cdots, u_p'$ be the new variables and $\theta_m(u')$ a θ of order m belonging to A if m is positive or the inverse of a θ of order $-m$ if m is negative. Let

finally $\psi(u')$ be the transformed of ϕ. The meromorphic function

$$\theta_m^{-1}(u')\cdot\phi(u) = \theta_m^{-1}(u')\psi(u') = \chi(u')$$

behaves like an intermediary function belonging to A with a fundamental form identically zero. By considering the relations for the corresponding coefficients $\alpha_{j\mu}$, it is found that $\alpha_{j\mu} = \alpha_{\mu j}$ $(\mu, j \leqq p)$. Hence the product of χ by a suitable quadratic exponential behaves in a similar manner with $\alpha_{j\mu} = 0$ $(j, \mu \leqq p)$. The relations satisfied by the other (α)'s show that they are also zero. Hence, if $\alpha'_{j\mu}$, $\alpha''_{j\mu}$ correspond to $\theta_m(u')$, and to $e^{G(u')}\cdot\psi$, where the exponential is the one already mentioned, we shall have $\alpha'_{\mu\nu} = \alpha''_{\mu\nu}$ whence follows that the entire function $e^{G(u')}\cdot\psi$ behaves relatively to A like a θ-function. *It is therefore a theta of order* m, which proves our affirmation.

The integer m, which is the greatest common divisor of the coefficients of F, is also called the *order* of ϕ.

The dimension of the linear system to which θ_m belongs, or which is the same, of the one to which ϕ belongs, is the pfaffian of F',

$$\frac{m^p e_p^p}{\prod_\mu (e_p/e_\mu)} = m^p \cdot e_1 e_2 \cdots e_p = \pi'.$$

Let D be the unimodular transformation changing Ω into A. We have

$$\Phi' = \bar{D}^{-1}\Phi D^{-1}, \qquad F' = \bar{D}FD.$$

Hence

$$\pi' = D\pi.$$

Finally, if Δ, Δ' are the determinants formed with the real and imaginary terms of Ω and A, we have

$$\Delta' = D\Delta, \qquad \therefore \ \pi\Delta = \pi'\Delta' < 0.$$

Thus, as shown by Bagnera and de Franchis in the case $p = 2$, the pfaffians of the non-degenerate fundamental forms of Ω all have the sign of $-\Delta$. By applying to Ω a suitably chosen unimodular transformation, we can arrange matters so that they will all be positive. The dimension of a complete linear system of intermediary functions will then be exactly equal to the corresponding pfaffian.

§ 4. The relation $\rho = 1 + k$. Theorem of Appell-Humbert

69. Let Φ_1 be a principal form, $\Phi_2, \Phi_3, \cdots, \Phi_{k+1}$ other alternate forms of Ω constituting with the first a set of $k+1$ independent forms. The conditions that $x\Phi_1 + y\Phi_j$ be principal, $(x, y$ are integers), can be expressed in the form of inequalities

$$f_1(x, y) > 0, \qquad f_2(x, y) > 0, \qquad \cdots, \qquad f_n(x, y) > 0,$$

where the (f)'s are homogeneous polynomials with integral coefficients. These conditions, which are satisfied for $x = 1$, $y = 0$, will certainly also be when we take $y = 1$, and x great enough. Hence, if Φ_j is not principal, we can always replace it in the above system by a principal form. This will allow us to assume that all the (Φ)'s are principal forms. To Φ_j correspond non-degenerate intermediary functions, hence a fundamental form F_j, of genus p, inverse of Φ_j. Let us represent any alternate form G of genus p by the point (G) of a space $S_{p(2p-1)-1}$ having its coefficients for homogeneous coördinates. The relation between a form and its inverse establishes an involutory birational correspondence between the points of this space, and if G is not degenerate, the point (G) is not fundamental for that correspondence. Let Φ, F be a principal form and the corresponding fundamental form. The S_k which contains the points (Φ) is transformed by the involution into an algebraic k-dimensional variety W_k containing all the (F)'s. I say that there is no W_h, $h < k$, containing all these last points. For otherwise there would be a variety W'_h containing all the (Φ)'s, hence all the points $\alpha\Phi + \beta\Phi_j$, where α, β are arbitrary positive integers. In the neighborhood of (Φ) there would then be found within W'_h a point-set, everywhere dense, not contained in a space of less than k dimensions, which would have as a consequence effectively $h \geqq k$.

It follows that the points (F) are not contained in a space of less than k dimensions. Besides, if F, F' are two fundamental forms, $\alpha F + \beta F'$ is another fundamental form (α, β, arbitrary positive integers). Hence if W_k were not an S_k, it would have to contain an infinity of straight lines passing through an ordinary point not situated within an S_k which is impossible. It follows that W_k is merely an S_k.

Let finally F' be a degenerate fundamental form of genus $p' < p$. There corresponds to it an intermediary function in p' variables. We know that there exists then at least one intermediary function ϕ'', of genus $p'' = p - p'$, such that $\phi'^{\alpha}\,\phi''^{\beta}$ be of genus p, where α, β are arbitrary positive integers. If F'' is the fundamental form corresponding to ϕ'', $(\alpha F' + \beta F'')$ will be in the space S_k containing the points which correspond to the non-degenerate forms. Hence (F') will also belong to that S_k.

Thus the fundamental forms like the Riemann forms give rise to a linear system ∞^k.

The modulus generated by the fundamental forms will have a minimum base composed of $k + 1$ forms $F_1, F_2, \cdots, F_{k+1}$. Let F be a fundamental form of genus p corresponding to intermediary functions of order one. The coefficients of F will then be prime to each other, and there exists a minimum base for fundamental forms of which F is an element. Assume then $F = F_1$. The form $F'_j = F_j + xF_1$ (x a positive integer) is not degenerate for x

arbitrary, even if F_j is. If F_j is degenerate, we can then replace it by F'_j, and we thus see that there exists a minimum base for fundamental forms composed of non-degenerate forms. We shall assume that the above minimum base already has this property.

70. Let us prove now the following important

THEOREM: *The non-degenerate intermediary functions of a complete continuous system of such functions cut out a complete continuous system of hypersurfaces.*

Let us reduce Ω to a canonical matrix A in such a manner that the intermediary functions in question become (θ)'s belonging to A. We have then to prove that the (θ)'s of a given order m cut out a complete continuous system. Let us represent V_p, as before, by equations

$$\tau x_j = \theta_n^j \left[\begin{smallmatrix} g \\ h \end{smallmatrix}\right](u) \qquad (j = 1, 2, \cdots, s)$$

where $s - 1$ is the dimension of the (θ)'s of order n of given characteristic. We assume that this representation furnishes a non-singular V_p in point to point correspondence without exception with U_{2p}.

Let $\{C_m\}$ be the complete system of hypersurfaces of V_p containing as total hypersurfaces those cut out by the θ_m. We have to show that an arbitrary C_m can be cut out by a θ_m.

Let us designate by $|H|$ the system of hyperplane sections. Since V_p is without singularities, an arbitrary hypersurface lH of the complete system $|lH|$, (l great enough), can be cut out in the S_{s-1} containing V_p by a polynomial of order l.*

If we substitute in this polynomial the (θ)'s in place of the (x)'s, we find that every hypersurface of lH can be cut out by a θ_{nl}. But by means of an ordinary transformation of V_p, every linear system of $\{C_{nl}\}$ can be transformed into another containing an arbitrarily assigned linear system, since these systems are all representable by the points of a Picard variety of period matrix isomorphic to Ω, and which is the image of an involution on V_p. It follows that all the linear systems in question have the same dimension, equal to that of a θ_{nl} of given characteristic. This proves the proposition for $\{C_{nl}\}$, when l is above a certain limit.

We conclude from this that every rC_m, (r a sufficiently high multiple of n), is cut out by a θ_{mr}. In the neighborhood of an arbitrary point (u^0) of C_m we shall have

$$\theta_{mr}(u) = [f(u_1, u_2, \cdots, u_p)]^r \cdot g(u_1, u_2, \cdots, u_p),$$

where f is a polynomial in $u_p - u_p^0$ whose coefficients are holomorphic in $u_1, u_2, \cdots, u_{p-1}$, in the neighborhood of the set of values $u_1^0, u_2^0, \cdots, u_p^0$, and g is holomorphic in the neighborhood of (u^0), with $g(u_1^0, u_2^0, \cdots, u_p^0) \neq 0$.

*Severi, Rendiconti di Palermo, vol. 28 (1909), pp. 33–87.

Hence $\theta_{mr}^{1/r}$ is holomorphic in the vicinity of (u^0) and therefore it is an entire function. Besides, it behaves like a θ_m with respect to the matrix A, hence up to an exponential quadratic factor perhaps, it is a θ_m which cuts out C_m and the theorem is proved.

71. The preceding theorem will lead us rapidly to the value of ρ. Returning to the minimum base $F_1, F_2, \cdots, F_{k+1}$, for the fundamental forms, let ϕ_i be the non-degenerate intermediary function corresponding to F_i, and C_i the hypersurface which it cuts out. I say that we cannot have a relation such as $\sum \lambda_i C_i = 0$. Indeed, let $\lambda_i = \lambda_i' - \lambda_i''$ where the (λ')'s and the (λ'')'s all are positive integers. By definition, there exists a hypersurface E such that $D' = E + \sum \lambda_i' C_i$ and $D'' = E + \sum \lambda_i'' C_i$ are total hypersurfaces of the same continuous system. E can be replaced by any hypersurface of a continuous system which contains it. Hence, we can always consider it as being cut out by an intermediary function ϕ of order m, high enough, belonging to a fundamental form mF of genus p. For a suitable choice of m, the fundamental forms $mF + \sum \lambda_i' F_i$, $mF + \sum \lambda_i'' F_i$ are not degenerate, and the intermediary functions $\phi\Pi_i \phi_i^{\lambda_i'}$, $\phi\Pi_i \phi_i^{\lambda_i''}$ will not be so either. Since the hypersurfaces D', D'' which they cut out belong to the same continuous system, this must also be true for the functions in question and their fundamental forms must coincide—that is, we must have

$$\sum \lambda_i F_i = 0.$$

Hence $\lambda_1 = \lambda_2 = \cdots = \lambda_{k+1} = 0$, and the (C)'s are effectively independent.

An immediate corollary is that we must have $\rho \geqq k + 1$, and since

$$\rho \leqq k + 1,$$

it follows that $k + 1$ *and* ρ *are equal,* a result whose importance is obvious. Incidentally, we have shown that the (C)'s form a base for the hypersurfaces of V_p.

72. THEOREM OF APPELL-HUMBERT: *Every hypersurface of* V_p *may be cut out by an intermediary function.**

Let C be an arbitrary hypersurface of V_p. We have $\lambda C + \sum \lambda_i' C_i = \sum \lambda_i'' C_i$ (λ, λ_i', λ_i'', positive integers). Hence as before there are two hypersurfaces D', D'' cut out by non-degenerate intermediary functions, and such that $\lambda C + D'$ and D'' belong totally to the same complete continuous system. Hence there are two intermediary functions ϕ, ϕ' cutting out $\lambda C + D'$ and D'. The function $\psi = \phi/\phi'$ behaves like an intermediary function relatively to the periods. Besides D' may be taken arbitrarily within its continuous system. Let D_1' be another hypersurface of that system. There exist inter-

*See Humbert, Journal de mathématiques pures et appliquées, ser. 4, vol. 9 (1893), pp. 29–170, for the case $p = 2$.

mediary functions ϕ_1, ϕ_1' cutting out $\lambda C + D_1'$ and D_1' and we see at once that $(\phi \cdot \phi_1')/(\phi' \cdot \phi_1)$ is neither zero nor infinite on any hypersurface of V_p. Hence $\psi_1 = \phi_1/\phi_1' = e^{G(u)} \cdot \psi$, where G is an entire function. Since we may always so choose D_1' that ψ_1 be holomorphic at a given point (u^0), ψ is an entire function—therefore it is an intermediary function. Thus λC is cut out by an intermediary function ψ. We may now show as in No. 70 that $\psi^{1/\lambda}$ is an intermediary function cutting out C, even if ψ is degenerate, which proves the theorem.

73. Let F and C be respectively the fundamental form and the hypersurface corresponding to ψ. We have $F + \sum \lambda_i' F_i = \sum \lambda_i'' F_i$ (λ_i', λ_i'', positive integers). Just as before there exists here a non-degenerate fundamental form F', such that $F' + F + \sum \lambda_i' F_i = F' + \sum \lambda_i'' F_i$ is not degenerate either. Let ϕ be an intermediary function belonging to F'. The intermediary functions $\psi\phi\Pi_i \phi_i^{\lambda_i'}$, $\phi\Pi_i \phi_i^{\lambda_i''}$ belong to the same continuous system of such functions, which leads at once to the relation $C = \sum (\lambda_i'' - \lambda_i') C_i$. Thus C_1, C_2, $\cdots$, C_{k+1} form a *minimum base*. Incidentally, these hypersurfaces are independent, hence $\sigma = 1$, as we have already found before in a different manner.

74. *Remarks.* I. When $p = 3$, we can arrive much more rapidly at the relation $\rho = 1 + k$. Indeed, we shall show below independently from this relation, that the arithmetic genus of an Abelian variety of genus p is equal to $(-1)^{p-1}$, hence when p is odd it is equal to the geometric genus. It follows in particular that V_3 is completely regular, in which case (No. 36) every two-cycle with zero periods for the integrals of the first kind, is algebraic, which gives at once $\rho = 1 + k$.

II. Whatever Ω, the p-uple integral of the first kind of V_p has at least one non-zero period since Ω is an array of rank p. We can then apply the theorem of No. 36: Every algebraic surface which is a complete intersection in V_p of hypersurfaces belonging to a sufficiently general linear system has for bases the traces of the bases of V_p.

III. Let us mention explicitly that, whatever p,

$$\rho_0^2 = \rho_0 = R_2 - \rho = R_2 - (1 + k) = p(2p - 1) - 1 - k.$$

§ 5. Formula for the arithmetic genera

75. In a paper in the Annals of Mathematics of 1916 the author has established this result: If $C = \sum_{i=1}^{s} \lambda_i C_i$, the arithmetic genus of C is given by

$$[C] = [\prod_{i=1}^{s} (1 + C_i)^{\lambda_i} - 1] - \binom{\sum \lambda_i - 1}{p - 1},$$

where at the right one must expand in series, then replace the non-numerical

terms of degree $\leqq p$ by the corresponding arithmetic genera. He has besides established a formula according to which $[(lC)^k]$ is a polynomial in l with coefficients of the first degree in $[C^i]$.

Assume now that C is a hypersurface cut out by an intermediary function of non-degenerate form F. If C is generic in its continuous system, V_p may be birationally transformed into a variety V'_p, non-singular and having for hyperplane sections the complete system $|lC|$ (l sufficiently great). The dimension of the containing space is $\pi l^p - 1$, where π is the pfaffian of F. On the other hand, the postulation of V'_p with respect to the varieties of order n of its space is $\pi(ls)^p$. Hence (Severi, loc. cit.),

$$\pi(ls)^p = \binom{s+p}{p}[(lC)^p] - \binom{s+p-1}{p-1}([(lC)^p] + [(lC)^{p-1}] - 1) + ([(lC)^{p-1}] + [(lC)^{p-2}])\binom{s+p-2}{p-2} + \cdots + (-1)^p([(lC)] + [V_p]).$$

If in these expressions the quantities $[(lC)^k]$ are replaced by their expressions in terms of genera $[C^i]$ we obtain an algebraic equation verified for an infinite number of sets of values (s, l) which cannot be thus related. The relation obtained must therefore be an identity. Making $l = 1$, we have for every value of s

$$\pi s^p = \left[\binom{s+p}{p}C^p - (C^p + C^{p-1} - 1)\binom{s+p-1}{p-1} + \cdots + (-1)^p(C + V_p)\right].$$

Moreover we can always find constants t_i such that, whatever s,

$$s^p = \sum_{i=0}^{p} t_i \binom{s+i}{i}.$$

By comparing the two values of s^p it is found that

$$[C] = (-1)^{p-1}[\pi(t_1 + t_2 + \cdots + t_p) - 1].$$

Making successively $s = 0$ and $s = -1$ in the preceding formula, we obtain $t_0 + t_1 + \cdots + t_p = 0, t_0 = (-1)^p$, whence ultimately $[C] = \pi + (-1)^p$. Finally, substituting $s = 0$ in the formula for πs^p, we find $[V_p] = (-1)^{p-1}$. *Thus the arithmetic genus of an Abelian variety of rank one and genus p is equal to $(-1)^{p-1}$.* This is in agreement with the value -1 already known for the arithmetic genus of hyperelliptic surfaces.

It is interesting to observe that a certain formula predicted by Severi but for which no proof is known as yet, is verified in the case of Abelian varieties.

Designating as before by i_s the number of s-uple integrals of the first kind, we must have according to this formula

$$[V_p] = i_p - i_{p-1} + \cdots + (-1)^{p-1} i_1.$$

Since $i_s = \binom{p}{s}$ and

$$1 - \binom{p}{1} + \binom{p}{2} - \cdots + (-1)^{p-1} \cdot p = (1-1)^p - (-1)^p = (-1)^{p-1},$$

the formula holds here.

76. Let F_i be the fundamental form of C_i. The pfaffian π will be a polynomial in $\lambda_1, \lambda_2, \cdots$, whose coefficients are simultaneous invariants of the forms F_i. Since

$$\pi + (-1)^p = [\prod_i (1 + C_i)^{\lambda_i} - 1] - \binom{\sum \lambda_i - 1}{p-1},$$

whatever the positive integers λ_i, this relation is an identity and the coefficients of the powers of the (λ)'s must be equal on both sides. Comparing those of $\lambda_1, \lambda_2, \cdots, \lambda_s$ we obtain $[C_1 C_2 \cdots C_s] = + G_s$, where G_s is a simultaneous invariant of the fundamental forms, $F_1, F_2, \cdots, F_s$ of which it is not necessary to give here the expression, which is easy enough to obtain. This formula solves the problem of the determination of the arithmetic genus for the complete intersections in V_p.

We verify in particular that

$$[C^p] = \pi \cdot p!, \qquad \text{(formula of No. 66; Poincaré)}$$

$$[C^{p-1}] = 1 + \frac{1}{2}\pi(p-1)\cdot p!$$

$$[C^{p-2}] = -1 + \frac{\pi(p-2)(3p-5)}{4!} \cdot p!, \qquad \text{etc.}$$

For $p = 2$, $[C^2], [C], [C_1 C_2]$ have precisely the values already obtained by Bagnera and de Franchis.

Chapter II. Abelian Varieties with Complex Multiplication

§ 1. Generalities

77. In the first chapter we have established the identity between the numbers ρ and $1 + k$. The next problem of interest is that of the determination of the numbers h, k for a wide range of cases. The varieties with complex multiplication will furnish them readily.

In order that the transformation T

$$(1) \qquad u'_j = \sum_{k=1}^{p} \lambda_{jk} u_k \qquad (j = 1, 2, \cdots, p),$$

define an algebraic correspondence on the Abelian variety of rank one V_p, belonging to the matrix Ω, it is necessary and sufficient (Humbert, Scorza) that there exist relations

$$\sum_k \lambda_{jk}\,\omega_{k\mu} = \sum_{\nu=1}^{2p} b_{\nu\mu}\,\omega_{j\nu} \tag{2}$$

$$(j = 1, 2, \cdots, p;\ \mu = 1, 2, \cdots, 2p),$$

where the (b)'s are rational numbers. These relations can also be written symbolically:

$$\|\lambda_{jk}\| \cdot \Omega = \Omega \cdot \|b_{\mu\nu}\|.$$

If the so-called "multipliers" as defined below are rational and equal, T is said to be an *ordinary multiplication* of V_p, while in the contrary case it is said to be a *complex multiplication* of the variety. If the determinant $|\lambda_{jk}| = 0$ we have to deal with a complex multiplication of an Abelian variety of genus $< p$ contained in V_p. We shall assume then in general that this determinant is not zero. Besides, (Frobenius) $|\lambda_{jk}| \cdot |\bar{\lambda}_{jk}| = |b_{\nu\mu}|$, and the rank of the determinant at the right is double that of $|\lambda_{jk}|$. Hence, if one is not zero, neither is the other. *Moreover, the determinant of the (b)'s is necessarily positive.* Let us assume that the (b)'s are integers. The determinant is then equal to a certain integer m and we have to deal with a correspondence $(1 - m)$. In order that we have a birational transformation, it is necessary and sufficient that the determinant be equal to one.

The *multipliers* of T already alluded to are simply the roots of the equation in α,

$$|\lambda_{jk} - \epsilon_{jk}\cdot\alpha| = 0 \qquad (\epsilon_{jj} = 1,\ \epsilon_{jk} = 0 \text{ if } j \neq k),$$

If none of them are zero, we have a multiplication of functions of genus p or *non-singular* multiplication.

According to Frobenius,

$$|\lambda_{jk} - \epsilon_{jk}\cdot\alpha| \cdot |\bar{\lambda}_{jk} - \epsilon_{jk}\cdot\alpha| = |b_{\nu\mu} - \epsilon_{\nu\mu}\cdot\alpha| = F(\alpha),$$

hence the multipliers are roots of an equation of degree $2p$, with rational coefficients, $F(\alpha) = 0$, called the *characteristic equation* of the complex multiplication T. A real root must annul each factor on the left side above and is therefore double for $F(\alpha)$. On the contrary, if a multiplier is imaginary its conjugate annuls the second factor on the left and the two may be simple roots of $F(\alpha)$. When the multiplication is singular, $F(\alpha)$ has zero roots and the determinant $|b_{\nu\mu}| = 0$. The characteristic equation whose properties from the point of view that interests us here, have been thoroughly studied by Frobenius, will play a fundamental part in the sequence. The problem which we propose to consider is the following: *Given a certain equation with rational*

coefficients, to find the most general Abelian varieties possessing a complex multiplication of which this equation is the characteristic equation, and to determine their invariants.

When the equation is arbitrary, the problem is far from simple, especially since a given Abelian variety may possess multiplications of widely different types. Now we have seen at the beginning of Part II that the problem of the determination of the numbers h, k, and therefore also of ρ, reduces itself to the following two problems: (a) To find the invariants of a pure matrix; (b) To find the simultaneous index of two pure matrices. We shall see that every complex multiplication belonging to a pure matrix has a characteristic equation of type $[f(\alpha)]^r = 0$, ($f(\alpha)$ irreducible), and it is the investigation of extensive cases where the characteristic equation is of this type that will occupy us very largely in the sequence.

78. We recall here, first, the point of view and method which Scorza followed in introducing the index h. Let T' be another complex multiplication than T and let

$$u'_j = \sum_{k=1}^{p} \lambda'_{jk}\, u_k, \qquad \sum_{k=1}^{p} \lambda'_{jk}\, \omega_{k\mu} = \sum_{\nu=1}^{2p} b'_{\nu\mu}\, \omega_{j\nu} \qquad (j = 1, 2, \cdots, p;\ \mu = 1, 2, \cdots, 2p)$$

be its equations. Whatever the rational numbers m, m', the equations $u'_j = \sum_k (m\lambda_{jk} + m'\lambda'_{jk})\, u_k$ define a new multiplication, since the relations $\sum_k (m\lambda_{jk} + m'\lambda'_{jk})\, \omega_{k\mu} = \sum_\nu (mb_{\nu\mu} + m'\, b'_{\nu\mu})\, \omega_{j\nu}$ are verified. This new multiplication will be designated by $mT + m'\, T'$.

Since the rank of the determinant $|b_{\nu\mu}|$ is equal to the sum of the ranks of the determinants $|\lambda_{jk}|$, $|\overline{\lambda}_{jk}|$, the ($b$)'s cannot all be zero without this being the case for all the (λ)'s and conversely. If the terms of a multiplication are all zero we shall write $T = 0$. It is clear that, given $4p^2$ multiplications, we can find a linear combination of them identically zero, hence multiplications form a finite modulus, and in fact the base number is $1 + h$.—This fundamental point is proved by Scorza as follows: Consider the elements of any row of Ω as homogeneous point coördinates in an S_{2p-1}. To the p rows correspond p points which define an S_{p-1}. The equations (2) show that the projectivity with rational terms $B = ||b_{\nu\mu}||$, of S_{2p-1}, transforms the S_{p-1} into itself. Conversely a projectivity with rational terms having this property defines a multiplication of V_p. B is said to be a *Riemann projectivity* of Ω. If B' corresponds thus to T', to the multiplications $mT + m'\, T'$ and TT' correspond the respective Riemann projectivities $mB + m'\, B'$ and BB'. Hence in particular the base numbers for the projectivities and for the multiplications are the same. Now a bilinear form of Ω defines a reciprocity of S_{2p-1} with rational terms, or "a rational reciprocity," which transforms each point of the above S_{p-1} into an S_{2p-2} passing through that S_{p-1}. Let C, D, be two such

reciprocities; $C^{-1}D$ is a Riemann projectivity of Ω and defines therefore a multiplication. Conversely to the Riemann projectivity B corresponds the rational reciprocity BC, from which follows readily that there are exactly $1+h$ distinct multiplications of which no linear combination is a zero multiplication. A very simple discussion shows that $1+h \leqq 2p^2$, $1+k \leqq p^2$, and that if Ω is pure, $1+h \leqq 2p$, $1+k \leqq 2p-1$. We see that if $k>0$ there is at least one complex multiplication.

We recall again that every Riemann matrix is isomorphic to one of the type

$$\text{(I)} \qquad \left\| \begin{matrix} \omega_1, & 0, & \cdots, & 0 \\ 0, & \omega_2, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & \cdot & \cdots, & \omega_n \end{matrix} \right\|$$

where the (ω)'s are pure Riemann matrices not isomorphic to each other or else are of the type

$$\text{(II)} \qquad \left\| \begin{matrix} \omega, & 0, & \cdots, & 0 \\ 0, & \omega, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & \cdot & \cdots, & \omega \end{matrix} \right\|$$

where ω is pure. Of course we assume that two submatrices ω_i, ω_j, which enter into the type (I) are not composed with isomorphic pure matrices ω in case they are impure.

By considerations such as the above, Scorza has shown that if two Riemann matrices possess a simultaneous form, they possess isomorphic submatrices, these conditions being moreover necessary. The matrices ω_i in (I) do not possess therefore any simultaneous forms and if h_i, k_i are their invariants we have for Ω, if of type (I),

$$1+h = \sum (1+h_i), \qquad 1+k = \sum (1+k_i),$$

while for a matrix of type (II), with n terms in the main diagonal,

$$1+h = n^2(1+h'), \qquad 1+k = \frac{n(n-1)}{2}(1+h') + n(1+k'),$$

where h', k' are the invariants of ω. Hence, to find h, k, or ρ, it is sufficient to reduce Ω to the type (I) and to find the invariants h, k of certain pure matrices.

By considering the representative spaces, we see at once that:

(*a*) Every Riemann projectivity operates separately on the submatrices ω_i. This is an immediate consequence of the fact that the reduction to the type (I) is unique (Scorza).

(*b*) The characteristic polynomial $F(\alpha)$ corresponding to a Riemann pro-

jectivity is a product $f_1, f_2, \cdots, f_n$, where f_i is the characteristic polynomial of the projectivity corresponding to ω_i.

79. Let B be a Riemann projectivity of Ω. Its various powers, $B^0 = 1$, $B, \cdots, B^m, \cdots$ are also such projectivities. The degree of an equation $f(B) = 0$, (f a polynomial with integral coefficients) satisfied by these powers has a minimum q, and there exists a unique equation of this degree satisfied by B—it is the *minimum equation* of Frobenius.*

The integer q will be called the *degree* of B.

The equations $F(\alpha) = 0$, $f(\alpha) = 0$, have the same roots, hence if $f(0) = 0$, B is singular, and conversely. When the roots of $f(\alpha) = 0$ are all simple, B is said to be a *general* projectivity. In the contrary case, it is said to be *special*. A projectivity is general or special according as the space of minimum dimension containing its stationary points is or is not of dimensionality $2p - 1$. We shall see below that if B is special Ω is impure. For the present, let us show that *if B is general, non-singular, with irreducible minimum equation, its degree q divides* $1 + h$. For, first, there exists a matrix C such that $C^{-1}BC$ is a matrix with terms on one side of the principal diagonal all equal to zero, those of the diagonal itself being the roots of $F(\alpha)$ each taken with its multiplicity. From this it follows readily that the roots of the characteristic equation of $\psi(B)$ (ψ a polynomial with rational coefficients) are the numbers $\psi(\alpha_i)$, where α_i is any root of $F(\alpha)$. Hence in the first place, if ψ is of degree $< q$, $\psi(B)$ is not singular.

Let now A be a projectivity independent of the powers of B. I say that the projectivities $1, B, B, \cdots, B^{q-1}, A, AB, \cdots, AB^{q-1}$, are all independent. For otherwise there would have to be a relation $\phi(B) + A \cdot \psi(B) = 0$, where ϕ, ψ are of degree $q - 1$ at most. It is easy to see that since $\psi(B) \not\equiv 0$, there exists a projectivity $\chi(B) = \sum a_s B^s$, such that $\psi(B) \cdot \sum a_s B^s = m$, where m is a non-zero integer. Indeed the computation of the coefficients a_s is formally the same as that which presents itself when given an algebraic number α such that $\psi(\alpha) \neq 0$, it is proposed to put $1/(\psi(\alpha))$ in the form $(1/m)\sum a_s \alpha^s$, a problem which is easily solved. We would have then finally $mA = \phi(B)$, contrary to our assumption as to A. The $2q$ distinct projectivities B^s, AB^s are therefore effectively independent.

Let now A' be a projectivity independent of the preceding. One may show in a similar manner that the projectivities B^s, AB^s, $A'B^s$ ($s = 0, 1, \cdots, q - 1$) are independent, etc. Continuing thus there will come a time

* The term is due to Rosati, who in a note of the Torino Atti of May, 1916, investigated this equation more particularly from the point of view of its relations with correspondences on algebraic curves. There is also a recent note by Scorza bearing on the same subject in the Rendiconti dei Lincei of October, 1917.—(Added in 1922:—The results of this note have since been extensively exposed by Scorza in the Palermo Rendiconti, vol. 45 (1921), pp. 1–204. Not a few contacts with this part of our work are of course to be expected).

when we will have exhausted all the independent projectivities. As those obtained will have been grouped in sets of q, $1 + h$ is divisible by q. In particular, we observe that if $1 + h > q$, then certainly $1 + h \geqq 2q$.

80. We have said that if B is special, Ω is impure. This point is easy to prove. Let indeed $\phi(\alpha) = 0$ be the equation of which the roots of $F(\alpha)$ are simple roots. $\phi(\alpha)$ is of degree $< q$, hence $\phi(B)$ is a non-zero projectivity with multipliers all zero and therefore Ω, which possesses a singular projectivity, is necessarily impure. Similarly, if $F(\alpha) = F_1(\alpha) \cdot F_2(\alpha)$, where F_1, F_2 are irreducible and prime to each other, Ω is impure. For $F_1(B)$ is a Riemann projectivity of which some multipliers but not all are zero, hence it is a singular projectivity not identically zero, and Ω is impure.

We thus see that the characteristic equations of pure matrices are all of type $[f(\alpha)]^r = 0$, where f is irreducible of degree $q = 2p/r$, and $f(B) = 0$ is the minimum equation of B, so that its degree is also q.

It is interesting to notice that the impure matrices reducible to the type (II) of No. 78 possess at least one general projectivity. For if $u_1, u_2, \cdots, u_p$ are the variables corresponding to this matrix itself, its Abelian variety possesses the cyclic birational transformation of order n

$$u_i' = u_{p'+i} \qquad (p = n\,p';\ u_{p+i} = u_p).$$

The corresponding Riemann projectivity is cyclic, hence general.

Thus, amongst the matrices which possess a general projectivity are found those of type (II), whether pure or impure.

81. Let then B be a general Riemann projectivity with a characteristic equation $[f(\alpha)]^r = 0$, of degree $q = 2p/r$ with f irreducible. By making a change of variables, equations (1), (2) can be put in the form

$$u_j' = \alpha_j u_j; \tag{3}$$

$$\alpha_j \omega_{j\mu} = \sum_{\nu=1}^{2p} b_{\mu\nu} \omega_{j\nu} \qquad (j = 1, 2, \cdots, p;\ \mu = 1, 2, \cdots, 2p). \tag{4}$$

Let γ_1 be an arbitrary linear cycle of V_p, τ_{j1} the corresponding period of u_j. The equations (3), (4) show that $\tau_{11}\alpha_1, \tau_{21}\alpha_2, \cdots, \tau_{p1}\alpha_p$ form a system of simultaneous periods of $u_1, u_2, \cdots, u_p$, the corresponding cycle γ_2 being independent of γ_1. Similarly the quantities $\tau_{11}\alpha_1^{i-1}, \cdots, \tau_{p1}\alpha_p^{i-1}$ form a system of simultaneous periods belonging to a linear cycle γ_i of V_p and since $f(\alpha)$ is irreducible, the cycles $\gamma_1, \gamma_2, \cdots, \gamma_q$ are independent. If $r > 1$ there will be a cycle γ_{q+1} independent of the preceding with a period τ_{j2} for u_j. We shall have similarly cycles $\gamma_{q+1}, \cdots, \gamma_{2q}$, the period of u_j relatively to γ_{q+i} being $\tau_{j2}\alpha_j^{i-1}$. I say that between these $2q$ cycles, there

exists no homology. For otherwise there would have to be a relation

$$\frac{\tau_{j2}}{\tau_{j1}} = \frac{m_0 + m_1\,\alpha_j + \cdots + m_{q-1}\,\alpha_j^{q-1}}{m_0' + m_1'\,\alpha_j + \cdots + m_{q-1}'\,\alpha_j^{q-1}},$$

where the (m)'s and (m')'s are integers. From this would follow a relation with integral coefficients,

$$n\tau_{j2} = \tau_{j1}(n_0 + n_1\,\alpha_j + \cdots + n_{q-1}\,\alpha_j^{q-1}),$$

and therefore a homology between the cycles $\gamma_1, \gamma_2, \cdots, \gamma_{q+1}$, which is in contradiction to the assumption as to the independence of γ_{q+1} from the q other cycles. This reasoning can be continued and we shall obtain finally $2p$ independent cycles to which will correspond a period matrix Ω' isomorphic to Ω,

$$\Omega' = \| \tau_{j1}, \tau_{j1}\,\alpha_j, \tau_{j1}\,\alpha_j^2, \cdots, \tau_{j1}\,\alpha_j^{q-1}, \tau_{j2}, \tau_{j2}\,\alpha_j, \cdots, \tau_{jr}\,\alpha_j^{q-1} \| \quad (j = 1, 2, \cdots, p),$$

composed with the two arrays*

$$\tau = \| \tau_{j\mu} \|; \qquad \| 1, \alpha_j, \cdots, \alpha_j^{q-1} \| \quad (\mu = 1, 2, \cdots, r;\ j = 1, 2, \cdots, p).$$

82. The projectivity B being still general, assume now that $F(\alpha) = [f(\alpha)]^r \cdot F_1(\alpha)$, where $f(\alpha)$ is irreducible, of degree q, and prime to $F_1(\alpha)$. Of the multipliers, $\frac{1}{2}rq$, say $\alpha_1, \alpha_2, \cdots, \alpha_{\frac{1}{2}rq}$, are roots of $f(\alpha)$. Moreover, according to a remark made above, if $g(\alpha)$ is an arbitrary polynomial with rational coefficients, there exists a complex multiplication which may be represented by $g(T)$, with multipliers $g(\alpha_j)$ $(j = 1, 2, \cdots, p)$. There will then be rational numbers $b_{\nu\mu}$ such that

$$g(\alpha_j)\,\omega_{j\mu} = \sum_{\nu=1}^{p} b_{\nu\mu}\,\omega_{j\nu} \quad (j = 1, 2, \cdots, p;\ \mu = 1, 2, \cdots, 2p),$$

and the rank of the determinant $|b_{\nu\mu}|$ will be twice the number of expressions $g(\alpha_j)$ that are not zero. Let us take in particular $g(\alpha) = [f(\alpha)]^r$. We shall have

$$\sum_{\nu} b_{\nu\mu}\,\omega_{j\nu} = 0 \quad (\mu = 1, 2, \cdots, 2p;\ j = 1, 2, \cdots, \tfrac{1}{2}rq).$$

Hence $u_1, u_2, \cdots, u_{\frac{1}{2}rq}$ form a system of reducible integrals of the variety V_p belonging to Ω and T operates separately upon them. From this, we conclude that Ω is isomorphic to a matrix

$$\begin{Vmatrix} \Omega_1 & 0 \\ 0 & \Omega_2 \end{Vmatrix}$$

* For $r = 1$, p arbitrary, this reduction has already been indicated by Scorza in his Palermo Rendiconti paper of 1916, p. 24. For $r = p = 2$ it has been repeatedly used by Bagnera and de Franchis.

where Ω_1 is of genus $\frac{1}{2}rq$ and T operates separately upon it in correspondence with the characteristic equation $[f(\alpha)]^r = 0$, and upon Ω_2 with the equation $F_1(\alpha) = 0$. Ω_1 is therefore isomorphic to a matrix of type (II). By reasoning on Ω_2 as we have on Ω and continuing, we obtain finally the following result: Let $F(\alpha) = [f_1(\alpha)]^{r_1} \cdots [f_n(\alpha)]^{r_n}$ be the decomposition of $F(\alpha)$ into irreducible factors prime to each other. Ω is isomorphic to a matrix,

$$\begin{Vmatrix} \Omega_1, & 0, & \cdots, & 0 \\ 0, & \Omega_2, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots, & \Omega_n \end{Vmatrix},$$

where Ω_j (which is of type (II)) is transformed separately by T with the characteristic equation $[f_j(\alpha)]^{r_j} = 0$. Ω_j can be put in the form indicated in No. 81.

Let h_j, k_j, ρ_j, be the invariants of Ω_j. We have then at once (Scorza) the relations

$$1 + h = \sum (1 + h_j) + 2\sum \lambda_{jk},$$
$$1 + k = \sum (1 + k_j) + \sum \lambda_{jk},$$
$$\rho = \sum \rho_j + \sum \lambda_{jk},$$

where λ_{jk} is the simultaneous index of Ω_j and Ω_k. The last equation just written has already been obtained at the end of Part I.

It follows from our whole discussion that the determination of the invariants of any Riemann matrix is reducible to the following two problems: (*a*) To determine the invariants of a matrix such as Ω_j, that is possessing a general Riemann projectivity with characteristic equation of type $[f(\alpha)]^r = 0$ (f irreducible). (*b*) To determine the simultaneous index of two such matrices.

Let us observe that if Ω is of type (II), with T not operating separately upon the (ω)'s, and more especially if Ω is pure, then $n = 1$, and $F(\alpha)$ is the exact power of an irreducible polynomial, whose degree q is what we have called the degree of T. As closely related to all this we recall the two notes of Rosati and Scorza already referred to.

We recall again that if the simultaneous index of two matrices Ω and Ω' is not zero, they are isomorphic to two matrices, (Scorza)

$$\begin{Vmatrix} \Omega_1, & 0 \\ 0, & \Omega_2 \end{Vmatrix}, \qquad \begin{Vmatrix} \Omega_1, & 0 \\ 0, & \Omega_2' \end{Vmatrix}.$$

The problem which we propose to attack is the determination of h and k for a wide range of matrices with general projectivities, with special emphasis on pure matrices. Before we enter upon this task we shall add a last remark concerning the characteristic equation.

83. According to Frobenius* if T is a principal transformation, that is, a transformation which maintains identically invariant a principal form of Ω, the multipliers have all the same absolute value, say β. Assume that Ω is pure, which requires that $F(\alpha) = [f(\alpha)]^r$, where f is irreducible and of degree $q = 2p/r$. We shall have $\beta^{qr} = |b_{\nu\mu}|$. Moreover β^q is a rational number, hence the determinant $|b_{\nu\mu}|$ in this case is the exact power of a rational number. A real multiplier will then be equal to $\pm\beta$. If q is odd the multiplication T^q will possess a rational number for root of its characteristic equation. As the characteristic polynomial of T^q must still be the exact power of an irreducible polynomial, T^q will necessarily be an ordinary multiplication and $\alpha_j^q = \beta^q = m$, where m is a rational number. Hence, finally, $f(\alpha) = \alpha^q - m$. Thus the characteristic equation of a principal transformation of odd degree of a pure matrix is of the form $(\alpha^q - m)^r = 0$, (m a rational number).

84. *Permutable Projectivities.* According to Scorza, the transformation of coördinates

$$x_s = \sum_{j=1}^{p} \omega_{js} X_j + \sum_{j=1}^{p} \overline{\omega}_{js} X_{p+j}$$

reduces the equations of the projectivity B of S_{2p-1} to the form

$$\sigma X'_j = \sum_{h=1}^{p} \lambda_{hj} X_h; \qquad \sigma X'_{p+j} = \sum_{h=1}^{p} \overline{\lambda}_{hj} X_{p+h} \qquad (j = 1, 2, \cdots, p),$$

and since this transformation of coördinates is independent of the projectivity considered, it follows readily that if two projectivities are permutable, the same holds for the corresponding complex multiplications and conversely.

Let now $B_1, B_2, \cdots, B_s$ be permutable projectivities. The corresponding multiplications will also be permutable and the projectivities permutable with the (B)'s will be of type $\phi(B_1, B_2, \cdots, B_s)$, where ϕ is a polynomial with rational coefficients, of degree $q_i - 1$ at most in B_i (q_i is the degree of B_i). The system of projectivities $\phi(B_1, B_2, \cdots, B_s)$ is in every way analagous to the system of numbers of an algebraic domain. In particular, there exists a projectivity B_0, of degree q, such that any other is a linear combination of its powers.

Among the projectivities of the set, those with integer terms play the same part as its integers for an algebraic domain. Like these integers, they satisfy an equation whose first coefficient is unity, as follows from the fact that the roots of the minimum equation are also roots of the equation $F(\alpha) = 0$ which is of this nature. These roots are therefore algebraic integers and their symmetric functions are ordinary integers. The projectivities here considered possess therefore a minimum base with q terms $B_1, B_2, \cdots, B_q$.

*Journal für die reine und angewandte Mathematik, vol. 95 (1883), pp. 264–297.

A complex multiplication permutable with any other has necessarily all multipliers equal, their common value being an imaginary quadratic number α. Replacing if necessary Ω by a suitably chosen isomorphic matrix, we may assume that $\alpha = i\sqrt{d}$ (d a positive integer). The array τ can then be reduced to one with p rows and columns

$$\begin{Vmatrix} 1, & 0, & \cdots, & 0 \\ 0, & 1, & \cdots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdots, & 1 \end{Vmatrix}$$

and Ω is a matrix with p elliptic integrals, of the type called by Scorza "with *maximum indices*," for which $1 + h = 2(1 + k) = 2p^2$.

In general assume that for some general projectivity $F(\alpha) = [f(\alpha)]^r$ (f irreducible and of degree q), and that among the quantities $\alpha_1, \alpha_2, \cdots, \alpha_p$, are found $\frac{1}{2}q$ roots each taken r times, which requires that all roots of $f(\alpha)$ be imaginary. The array τ is then of the form

$$\begin{Vmatrix} \tau_1 \\ \tau_1 \\ \cdot \\ \cdot \\ \cdot \\ \tau_1 \end{Vmatrix}$$

where τ_1 is a square array of the same type as above with r rows and columns, and Ω is impure of type (II) composed r times with the matrix

$$\| 1, \alpha_j, \cdots, \alpha_j^{q-1} \| \qquad (j = 1, 2, \cdots, \tfrac{1}{2}q).$$

§ 2. Complex multiplication with irreducible characteristic equation.

85. As before, let $F(\alpha) = 0$ be the characteristic equation. We shall assume the roots $\alpha_1, \alpha_2, \cdots, \alpha_{2p}$ arranged in such order that $\bar{\alpha}_j = \alpha_{p+j}$ ($j < p$), and we propose to investigate the matrix

$$\Omega = \| 1, \alpha_j, \cdots, \alpha_j^{2p-1} \| \qquad (j = 1, 2, \cdots, p).$$

In order that it be a Riemann matrix there must exist an alternate Riemann form

$$\sum_{\mu=1}^{2p} c_{\mu\nu}\, x_\mu\, y_\nu. \tag{5}$$

This requires that

$$\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}(\alpha_j^{\mu-1}\alpha_k^{\nu-1} - \alpha_j^{\nu-1}\alpha_k^{\mu-1}) = 0 \quad (j, k = 1, 2, \cdots, p), \tag{6}$$

and that the Hermitian form

$$(7)\qquad \sum_{j,k=1}^{p} A_{jk}\, x_j\, \bar{x}_k; \qquad A_{jk} = -\frac{1}{4i}\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\,(\alpha_j^{\mu-1}\,\alpha_{p+k}^{\nu-1} - \alpha_j^{\nu-1}\,\alpha_{p+k}^{\mu-1}),$$

be definite positive.

Let G be the group of $F(\alpha) = 0$. The equation (6) will be verified when we replace the pair (α_j, α_k) by any pair of roots which may be derived from the pairs taken out of the set $\alpha_1, \alpha_2, \cdots, \alpha_p$ by the substitutions of G. On the other hand, in order that (7) be definite, it is necessary that none of the (A_{ii})'s be zero. Hence, as a necessary condition among the pairs of roots derived from those with indices both $\leqq p$ must not figure a pair of conjugate roots.

I say that this last condition is sufficient to insure that Ω be a Riemann matrix. For let $(\alpha_{j_1}, \alpha_{k_1}), \cdots, (\alpha_{j_s}, \alpha_{k_s})$ be the s pairs derived from those of indices $\leqq p$, $(\alpha_{j_1'}, \alpha_{k_1'}), \cdots, (\alpha_{j_t'}, \alpha_{k_t'})$, $(\alpha_1, \alpha_{p+1}), \cdots, (\alpha_p, \alpha_{2p})$, the $p + t$ pairs remaining with $s + p + t = p(2p - 1)$. Finally consider the equations in the unknowns $c_{\mu\nu}$:

$$(8)\qquad \sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\,(\alpha_{j_n}^{\mu-1}\,\alpha_{k_n}^{\nu-1} - \alpha_{j_n}^{\nu-1}\,\alpha_{k_n}^{\mu-1}) = 0 \quad (n = 1, 2, \cdots, s),$$

$$(9)\qquad \sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\,(\alpha_{j_n'}^{\mu-1}\,\alpha_{k_n'}^{\nu-1} - \alpha_{j_n'}^{\nu-1}\,\alpha_{k_n'}^{\mu-1}) = d_n \qquad (n = 1, 2, \cdots, t),$$

$$(10)\qquad -\frac{1}{4i}\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\,(\alpha_j^{\mu-1}\,\alpha_{p+j}^{\nu-1} - \alpha_j^{\nu-1}\,\alpha_{p+j}^{\mu-1}) = e_j \quad (j = 1, 2, \cdots, p).$$

The determinant of the coefficients is up to the sign

$$\left|\alpha_j^{\mu-1}\,\alpha_k^{\nu-1} - \alpha_j^{\nu-1}\,\alpha_k^{\mu-1}\right| \qquad (j, k, \mu, \nu = 1, 2, \cdots, 2p;\ j \neq k,\ \mu \neq \nu),$$

or the determinant formed with the minors of order two of the determinant of Vandermonde of $\alpha_1, \alpha_2, \cdots, \alpha_{2p}$, hence equal to a power of that determinant and therefore different from zero. It follows that there will be a unique solution for the (e)'s. Whether these coefficients are rational or not, we can consider the corresponding Hermitian form (7). It will be definite positive if the p roots of the equation in β,

$$|A_{jk} - \epsilon_{jk}\,\beta| = 0 \qquad (\epsilon_{jj} = 1;\ \epsilon_{jk} = 0, j \neq k)$$

are all positive. But when the (d)'s are all zero, these p roots are equal to the (e)'s, since (7) becomes then

$$\sum_{j=1}^{p} e_j\, x_j\, \bar{x}_j.$$

Hence when we take the (d)'s sufficiently small in absolute value and the (e)'s positive, the roots in question will all be positive and the Hermitian form will be definite positive.

Let us consider, as we have already had occasion to do, the (e)'s as homogeneous point coördinates in an $S_{p(2p-1)-1}$. The point whose coördinates satisfy the s equations (8) is contained in a *rational* $S_{p(2p-1)-s-1}$, by which we mean that the space contains $p(2p-1)-s$ independent points with rational coördinates. We can see this at once by observing that equations (8) are simply permuted among themselves by the substitutions of G and therefore have as many independent solutions in rational numbers as they have independent solutions in general. Their independence results from the fact that the array of the coefficients is composed of s rows taken from a non-zero determinant.

In the $S_{p(2p-1)-s-1}$ in question there will then be a rational point differing as little as we please from any given point and in particular from the point whose coördinates satisfy the equations (8), (9), (10), where the (d)'s are sufficiently small and the (e)'s positive. In these conditions $\sum c_{\mu\nu} x_\mu y_\nu$ will be a principal form of Ω, which proves our proposition.

Thus, given an irreducible equation of degree $2p$ with roots all imaginary, in order that there correspond to it a Riemann matrix Ω, it is necessary and sufficient that its group does not permute any pair of roots taken from a set of p roots among which none are conjugate to each other, with a pair of conjugate roots.

When Ω exists, $1+k$ is obviously equal to the number of independent solutions of the equations (8), that is $1+k=p(2p-1)-s=p+t$.

86. To determine h, we must find the number of independent rational solutions possessed by the equations in the unknowns $c_{\mu\nu}$,

$$\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\,\alpha_j^{\mu-1}\,\alpha_k^{\nu-1}=0 \qquad (j,k=1,2,\cdots,p).$$

This equation must be satisfied when α_j, α_k are permuted and also when they are replaced by any one of the pairs of roots $(\alpha_{j_n},\ \alpha_{k_n})$, $(\alpha_{k_n},\ \alpha_{j_n})$ $(n=1,2,\cdots,s)$; (α_j,α_j) $(j=1,2,\cdots,2p)$; whence the equations

$$\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\,\alpha_{j_n}^{\mu-1}\,\alpha_{k_n}^{\nu-1}=0, \qquad \sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\alpha_{k_n}^{\mu-1}\,\alpha_{j_n}^{\nu-1}=0 \qquad (n=1,2,\cdots,s),$$

$$\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}\alpha_j^{\mu+\nu-2}=0, \qquad (j=1,2,\cdots,2p).$$

The array of the coefficients is composed of $2(p+s)$ rows of the determinant

$$|\alpha_j^{\mu-1}\,\alpha_k^{\nu-1}| \qquad (\mu,\nu,j,k=1,2,\cdots,2p),$$

which is not zero. The above equations are therefore independent and as they are merely permuted by the substitutions of G, they will possess as many independent rational solutions as independent solutions in general. Hence, finally $1 + h = 4p^2 - 2p - 2s = 2(1 + k)$. Thus the invariants of Ω satisfy the relations $1 + h = 2(1 + k) = 2p(2p - 1) - 2s = 2(p + t)$.

87. The preceding result gives rise to some interesting observations. For we have seen that when a matrix is pure, $1 + h \leqq 2p$. Hence, in order that Ω be pure, it is necessary that $s \geqq p(2p - 1) - p$. On the other hand, the p pairs of roots (α_j, α_{p+j}) are not among the pairs $(\alpha_{j_n}, \alpha_{k_n})$ $(n = 1, 2, \cdots, s)$. Hence in order that Ω be pure, it is necessary that $s = p(2p - 1) - p$, which requires that *the only pairs that may not be derived from those of indices* $\leqq p$ *by the substitutions of* G, *are the pairs of conjugate roots.*

Let $z_1 = m_1\alpha_1 + m_2\alpha_2 + \cdots + m_{2p}\alpha_{2p}$ be a Galois function of $F(\alpha) = 0$, the (m)'s being arbitrary integers, and consider the Galois resolvent $\phi(z) = 0$ of which z_1 is a root. The (α)'s are rational functions of z_1 with real coefficients. Hence z_1 is not real, as can also be seen directly. Replacing z_1 by $\bar{z}_1$ in these rational functions, we obtain a substitution S, of order two of G, which has the property of permuting any two conjugate roots. Moreover, if another substitution S' had the same property, we would have $SS' = 1$, hence $S' = S^{-1} = S$ and therefore S is unique.

Let us now return to Ω. In order that it be a Riemann matrix and pure, it is necessary and sufficient: (a) That S be permutable with all the substitutions of G. (b) That among the corresponding roots, $\alpha_1, \alpha_2, \cdots, \alpha_p$, none be conjugate, and moreover that from the pairs (α_j, α_k) it be possible to derive all the pairs of non-conjugate roots by the substitutions of G. To begin with, the second condition is obviously necessary. Let us show that so is the first. For G must not permute the pairs of conjugate roots with pairs of roots that are not conjugate. Hence, if T is an arbitrary substitution of G and if $T\alpha_j = \alpha_k$ we must have $TS\alpha_j = S\alpha_k$, whence $S^{-1}TS = T$, and T is effectively permutable with S.

Let us show that our two conditions are also sufficient. For, if $T\alpha_j = \alpha_k$, we shall also have $T\bar{\alpha}_j = TS\alpha_j = ST\alpha_j = S\alpha_k = \bar{\alpha}_k$, and the pair $(\alpha_j, \bar{\alpha}_j)$ is permuted with $(\alpha_k, \bar{\alpha}_k)$; hence the pairs of conjugate roots are not permuted with any others by the substitutions of the group. The second condition insures then that $t = 0$, the pairs $(\alpha_j, \bar{\alpha}_j)$ being all alone excluded. The equations for the coefficients of an alternate Riemann form are here

$$\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}(\alpha_j^{\mu-1}\alpha_k^{\nu-1} - \alpha_j^{\nu-1}\alpha_k^{\mu-1}) = 0$$

$$(j, k = 1, 2, \cdots, 2p;\ j \neq p + k).$$

The quantities

$$A_{jj} = -\frac{1}{4i}\sum_{\mu,\nu=1}^{2p} c_{\mu\nu}(\alpha_j^{\mu-1}\alpha_{p+j}^{\nu-1} - \alpha_j^{\nu-1}\alpha_{p+j}^{\mu-1})$$

will not all be zero, for otherwise the (c)'s would also be zero. But if one of the quantities A_{jj} is zero, all the others will also be zero for they are transitively permuted by the substitutions of G. Hence none of them is zero and the Hermitian form corresponding to the arbitrary Riemann form considered becomes here $\sum_{j=1}^{p} A_{jj} x_j \bar{x}_j$, and is always of genus p. Hence finally every Riemann form of Ω is of genus p and this matrix is actually pure. This completes the proof.

Observe that the invariants of the pure matrix will be given by

$$1 + h = 2(1 + k) = 2p,$$

h having the maximum value which it may have for such a matrix.

88. A particularly interesting case is that where p is prime. Then Ω, which is of type (II), is certainly pure, whence the following result: Let $F(\alpha) = 0$ be an irreducible equation of degree $2p$ (p prime), with roots all imaginary. Either the group of the equation permutes only among themselves the pairs of conjugate roots, or else in every set of p roots there are at least two which are permutable with a pair of conjugate roots.

89. Let us endeavor to characterize $F(\alpha)$ when its group is permutable with S^* or, which is the same, when there is a corresponding pure matrix Ω. The group G merely permutes the equations in the unknowns d,

$$\bar{\alpha}_j = d_0 + d_1\alpha_j + \cdots + d_{2p-1}\alpha_j^{2p-1} \quad (j = 1, 2, \cdots, 2p),$$

and hence these equations possess a rational solution which besides is unique. This means that $\bar{\alpha}_j = Q(\alpha_j)$, where Q is a polynomial with rational coefficients independent of j. Thus every root can be expressed as a rational function, the same for all of them, of its conjugate. Conversely if $\alpha_j = Q(\alpha_j)$, whatever j, S and G are permutable. For denoting still by z_1 the Galois function, we shall have first

$$\alpha_j = R_j(z_1), \qquad \bar{\alpha}_j = Q[R_j(z_1)].$$

We may then obtain every substitution of G by replacing z_1 by a suitably chosen root z_2 of the Galois equation. If $T\alpha_j = \alpha_k$, we shall have

$$\alpha_k = T\alpha_j = R_j(z_2), \qquad \overline{T\alpha}_j = Q[R_j(z_2)] = Q(\alpha_k) = \bar{\alpha}_k,$$

that is, $TS\alpha_j = ST\alpha_j$, or $TS = ST$.

* From this property follows already that the solution of the characteristic equation is reducible to that of an equation of degree p followed by a quadratic, but this result is insufficient for some applications which we have in view.

Thus, in order that S and G be permutable, it is necessary and sufficient that whatever j, $\bar{\alpha}_j = Q(\alpha_j)$, where Q is a polynomial with rational coefficients independent of j.

But we can go still further. Indeed, the p points of an S_{2p-1} whose non-homogeneous point coördinates are $\alpha_j + \bar{\alpha}_j$, $\alpha_j^2 + \bar{\alpha}_j^2$, $\cdots$, $\alpha_j^{2p-1} + \bar{\alpha}_j^{2p-1}$ are certainly distinct, for if two of them had their first two coördinates equal, $F(\alpha)$ would have a double root. Given arbitrary integers $d_1, d_2, \cdots, d_{2p-1}$, the distances from these points to the corresponding hyperplane

$$d_1 x_1 + d_2 x_2 + \cdots + d_{2p-1} x_{2p-1} = 0$$

are therefore all different. Whence the following conclusion: If we set

$$\alpha_j' = d_1 \alpha_j + d_2 \alpha_j^2 + \cdots + d_{2p-1} \alpha_j^{2p-1},$$

the quantities $\alpha_j' + \bar{\alpha}_j'$ are all distinct. In other words Ω possesses a Riemann projectivity with irreducible characteristic equation and such that if its multipliers are still denoted by $\alpha_1, \alpha_2, \cdots, \alpha_p$, the p sums $2\zeta_j = \alpha_j + \bar{\alpha}_j$ are all distinct. If we adjoin ζ_j to the domain of rationality, the pair of conjugate roots $\alpha_j, \bar{\alpha}_j$ is determined in one and only one way, and their product $\alpha_j \bar{\alpha}_j$ is therefore a rational function of ζ_j. On the other hand the (ζ)'s are transitively permuted by the substitutions of G, hence they satisfy an irreducible equation $\psi(\zeta) = 0$ of degree p, and the characteristic equation is of the form

$$\prod_{j=1}^{p} (\alpha^2 - 2\zeta_j \alpha + R(\zeta_j)) = 0,$$

where R is a polynomial of degree $p-1$ with rational coefficients and such that $\zeta_j^2 < R(\zeta_j)$ $(j = 1, 2, \cdots, p)$. Of course these conditions are not sufficient to make certain that Ω is pure. For example, take the case $p = 2$. The characteristic equation is of the form

$$(\alpha^2 - 2\zeta_1 \alpha + m\zeta_1 + n)(\alpha^2 - 2\zeta_2 \alpha + m\zeta_2 + n) = 0,$$

where m, n are rational and ζ_1, ζ_2 are the two roots of an equation

$$a\zeta^2 + b\zeta + c = 0$$

with coefficients a, b, c, integers and $a > 0$. We must have $\zeta_j^2 < m\zeta_j + n$ $(j = 1, 2)$, which is equivalent to the inequalities

$$a(an + c)^2 - b(an + c)(am + b) + c(am + b)^2 > 0,$$
$$(am + b)(2na^2 - mab + 2ac - b^2) > 0.$$

Moreover, in order that Ω be pure, it is necessary that the pairs of conjugate roots be transitively permuted. This requires that $\alpha_1 \alpha_2 + \bar{\alpha}_1 \bar{\alpha}_2$ be irrational, a condition which is besides sufficient. A very simple calculation shows that

this is equivalent to requiring that

$$a[a(an+c)^2 - b(an+c)(an+b) + c(an+b)^2]$$

be not the square of a rational number.

When these conditions are satisfied, the matrix

$$\left\| \begin{matrix} 1, & \alpha_1, & \alpha_1^2, & \alpha_1^3 \\ 1, & \alpha_2, & \alpha_2^2, & \alpha_2^3 \end{matrix} \right\|$$

is a Riemann matrix and pure.

It is scarcely possible to go further when the equation $F(\alpha) = 0$ is arbitrary and so we shall pass on to the investigation of the particularly important case where it is Abelian, when the preceding results may be completed and much increased in precision.

(*To be continued*)